

# DATA TERMINAL EQUIPMENT AND DATA RE-ACQUIRING METHOD

Publication number: JP2003016288

Publication date: 2003-01-17

Inventor: HIGUCHI GOJI

Applicant: SANYO ELECTRIC CO

Classification:

- international: G06Q30/00; G06F12/14; G06F21/24; G06Q10/00;  
G06Q50/00; G10K15/02; H04L9/08; G06Q30/00;  
G06F12/14; G06F21/00; G06Q10/00; G06Q50/00;  
G10K15/02; H04L9/08; (IPC1-7): G06F17/60;  
G10K15/02; H04L9/08

- European:

Application number: JP20010199100 20010629

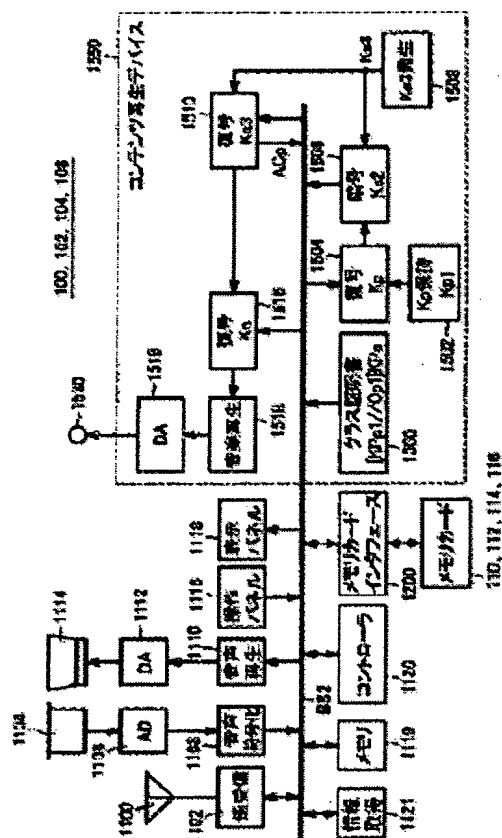
Priority number(s): JP20010199100 20010629

Report a data error here

## Abstract of JP2003016288

**PROBLEM TO BE SOLVED:** To provide data terminal equipment and a data re-acquiring method with which data terminal equipment acquiring copied contents data can easily re-acquire contents data received before.

**SOLUTION:** A memory 1119 stores a database registering information on a copy source. When the re-acquisition request of copied contents data is inputted through a control panel 1116, a controller 1120 of a portable telephone set 102 accesses a portable telephone set 100 of the copy source on the basis of the information on the copy source stored in the memory 1119 and when the copy of contents data is permitted in the portable telephone set 100, the contents data are re-acquired from the portable telephone set 100.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-16288

(P2003-16288A)

(43) 公開日 平成15年1月17日 (2003.1.17)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
G 0 6 F 17/60	3 0 2	G 0 6 F 17/60	3 0 2 E 5 J 1 0 4
	1 4 2		1 4 2
	3 3 6		3 3 6
	5 1 2		5 1 2
	Z E C		Z E C

審査請求 有 請求項の数 11 O L (全 33 頁) 最終頁に続く

(21) 出願番号 特願2001-199100(P2001-199100)

(22) 出願日 平成13年6月29日 (2001.6.29)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 発明者 樋口 剛司

大阪府守口市京阪本通2丁目5番5号 三

洋電機株式会社内

(74) 代理人 100064746

弁理士 深見 久郎 (外3名)

Fターム(参考) 5J104 AA01 AA16 EA01 EA04 NA02

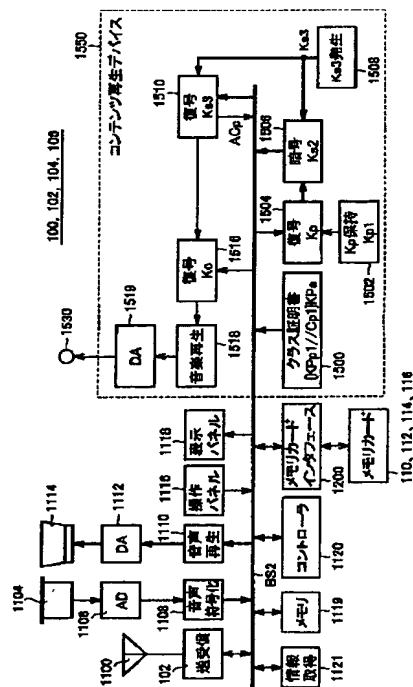
PA14

(54) 【発明の名称】 データ端末装置、およびデータ再取得方法

(57) 【要約】

【課題】 複製されたコンテンツデータを受信したデータ端末装置が以前に受信したコンテンツデータを容易に再取得できるデータ端末装置およびデータ再取得方法を提供する。

【解決手段】 メモリ1119は複製元に関する情報が登録されたデータベースを格納する。携帯電話機102のコントローラ1120は、複製されたコンテンツデータの再取得要求が操作パネル1116を介して入力されると、メモリ1119に格納された複製元に関する情報に基づいて複製元である携帯電話機100へアクセスし、携帯電話機100においてコンテンツデータの複製が許可されたとき、コンテンツデータを携帯電話機100から再取得する。



## 【特許請求の範囲】

【請求項1】 複製されたコンテンツデータと前記コンテンツデータの付加情報と前記コンテンツデータの複製元の固有情報とを含むデータを受信し、前記複製元に関する情報を管理するデータ端末装置であって、前記コンテンツデータを記録するデータ記録装置との間でデータのやり取りを行なうインタフェースと、外部とのデータのやり取りを行なう送受信手段と、前記複製元に関する情報を管理する情報管理手段と、前記データから前記コンテンツデータと前記固有情報と前記付加情報とを取得する取得手段と、制御手段とを備え、前記制御手段は、前記送受信手段を介して前記データを受信すると、その受信したデータを前記取得手段に与え、前記取得手段により取得されたコンテンツデータを前記インタフェースを介して前記データ記録装置に記録し、前記取得手段により取得された固有情報と付加情報とを前記複製元に関する情報として前記情報管理手段に格納する、データ端末装置。

【請求項2】 複製されたコンテンツデータおよび前記コンテンツデータの付加情報を含むデータと、前記コンテンツデータの複製元にアクセスするアクセス情報とを受信し、前記複製元に関する情報を管理するデータ端末装置であって、前記コンテンツデータを記録するデータ記録装置との間でデータのやり取りを行なうインタフェースと、外部とのデータのやり取りを行なう送受信手段と、前記複製元に関する情報を管理する情報管理手段と、前記複製元の固有情報を生成する情報生成手段と、前記データから前記コンテンツデータと前記付加情報とを取得する取得手段と、制御手段とを備え、前記制御手段は、前記送受信手段を介して前記データを受信すると、その受信したデータを前記取得手段に与え、前記送受信手段を介して受信したアクセス情報を前記情報生成手段に与え、前記取得手段により取得されたコンテンツデータを前記インタフェースを介して前記データ記録装置に記録し、前記情報生成手段によって生成された固有情報と前記取得手段により取得された付加情報とを前記複製元に関する情報として前記情報管理手段に格納し、前記情報生成手段は、前記与えられたアクセス情報を用いて前記固有情報を生成し、その生成した固有情報を前記制御手段に与える、データ端末装置。

【請求項3】 指示を入力するためのキー操作手段と、各種の情報を視覚情報としてユーザに表示する表示手段とをさらに備え、前記制御手段は、前記キー操作手段を介して入力された前記複製元に関する情報の表示要求に応じて、前記情報管理手段から前記複製元に関する情報を読出して前記表

示手段に与え、前記表示手段によって表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求が前記キー操作手段を介して入力されると、前記固有情報に含まれるアクセス情報を用いて前記複製元のデータ端末装置から前記コンテンツデータを再取得し、

前記表示手段は、前記複製元に対応する情報を表示する、請求項1または請求項2に記載のデータ端末装置。

【請求項4】 指示を入力するためのキー操作手段と、各種の情報を視覚情報としてユーザに表示する表示手段とをさらに備え、

前記情報管理手段は、前記複製元のデータ端末装置から受信したコンテンツデータの個数に応じた複数の複製元に関する情報を管理し、

前記制御手段は、前記キー操作手段を介して入力された前記複製元に関する情報の表示要求に応じて、前記情報管理手段から前記複数の複製元に関する情報を読出して前記表示手段に与え、前記表示手段によって表示された複数の複製元に関する情報のうちユーザによって選択された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求が前記キー操作手段を介して入力されると、前記固有情報に含まれるアクセス情報を用いて前記選択されたコンテンツデータの複製元のデータ端末装置から前記コンテンツデータを再取得し、前記表示手段は、前記複数の複製元に対応する情報を表示する、請求項1または請求項2に記載のデータ端末装置。

【請求項5】 前記制御手段は、前記複製元のデータ端末装置がコンテンツデータの複製に応じたとき、前記送受信手段を介して前記複製元のデータ端末装置から前記コンテンツデータを再取得する、請求項3または請求項4に記載のデータ端末装置。

【請求項6】 前記コンテンツデータは、ライセンス鍵によって暗号化された暗号化コンテンツデータであり、前記制御手段は、前記キー操作手段を介して入力された前記ライセンス鍵を含むライセンスの配信要求に応じて、前記ライセンスを保持するサーバへアクセスし、前記サーバから前記ライセンスを受信する、請求項1から請求項5のいずれか1項に記載のデータ端末装置。

【請求項7】 複製されたコンテンツデータと前記コンテンツデータの付加情報と前記コンテンツデータの複製元の固有情報とを含むデータを受信し、前記付加情報および前記固有情報を前記コンテンツデータの複製元に関する情報として管理するデータ端末装置において前記コンテンツデータを前記複製元のデータ端末装置から再取得するデータ再取得方法であって、前記受信した複製元に関する情報を表示手段に表示する第1のステップと、前記表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求を受付ける第

2のステップと、  
前記表示された複製元に関する情報に含まれる固有情報に基づいて再取得要求がなされたコンテンツデータの複製元にアクセスし、前記複製元のデータ端末装置から複製されたコンテンツデータを再取得する第3のステップとを含むデータ再取得方法。

【請求項8】 複製されたコンテンツデータおよび前記コンテンツデータの付加情報を含むデータと、前記コンテンツデータの複製元にアクセスするアクセス情報とを受信し、前記付加情報と前記受信したアクセス情報を用いて生成された前記複製元の固有情報とを前記複製元に関する情報として管理するデータ端末装置において前記コンテンツデータを前記複製元のデータ端末装置から再取得するデータ再取得方法であって、

前記受信した複製元に関する情報を表示手段に表示する第1のステップと、

前記表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求を受付ける第2のステップと、

前記表示された複製元に関する情報に含まれる固有情報に基づいて再取得要求がなされたコンテンツデータの複製元にアクセスし、前記複製元のデータ端末装置から複製されたコンテンツデータを再取得する第3のステップとを含むデータ再取得方法。

【請求項9】 前記第1のステップにおいて、前記複製元のデータ端末装置から受信したコンテンツデータの個数に応じた複数の複製元に関する情報を表示し、前記第2のステップにおいて、前記表示された複数の複製元に関する情報のうちユーザによって選択された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求が受けられる、請求項7または請求項8に記載のデータ再取得方法。

【請求項10】 前記第3のステップにおいて、前記複製元のデータ端末装置が前記コンテンツデータの複製を許可したとき、前記複製元のデータ端末装置から前記コンテンツデータを再取得する、請求項7から請求項9のいずれか1項に記載のデータ再取得方法。

【請求項11】 前記コンテンツデータは、ライセンス鍵によって暗号化された暗号化コンテンツデータであり、

前記ライセンス鍵を含むライセンスの配信要求を受付ける第4のステップと、

前記ライセンスを保持するサーバへアクセスし、前記サーバから前記ライセンスを受信する第5のステップとをさらに含む、請求項7から請求項10のいずれか1項に記載のデータ再取得方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システム

において用いられるデータ端末装置、およびデータ再取得方法に関するものである。

【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このような情報通信網上において音楽データや画像データ等の著作権者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとりて考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【0012】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【0014】また、携帯電話機のユーザは、受信した暗号化コンテンツデータを聴いてみて良かったので、その受信した暗号化コンテンツデータを友人にプレゼントしたい場合もある。その場合、携帯電話機のユーザは、受信した暗号化コンテンツデータを友人の携帯電話機へ送信することによって暗号化コンテンツデータを複製する。

【0015】友人の携帯電話機は、暗号化コンテンツデータを受信し、その受信した暗号化コンテンツデータを装着されたメモリカードに記録する。そして、友人は、プレゼントされた暗号化コンテンツデータを復号および再生するためのライセンスを配信サーバから取得する指示を自己の携帯電話機に与え、携帯電話機は、そのライセンスを配信サーバから受信してメモリカードに記録する。これによって、友人は、プレゼントされた暗号化コンテンツデータを復号および再生して聴くことができる。また、暗号化コンテンツデータを、友人の携帯電話機からコピーすることもできる。この場合はユーザが自

分の携帯電話機を操作して、友人の携帯電話機に回線を接続して、友人の携帯電話機のメモリカードに記録された暗号化コンテンツデータを自分の携帯電話機のメモリカードに複製する。この場合、暗号化コンテンツデータの複製は自由に行なわれるが、暗号化コンテンツデータをプレゼントされた／複製したユーザは、そのままでは暗号化コンテンツデータを復号および再生できず、配信サーバから暗号化コンテンツデータを復号および再生するためのライセンスを購入する必要がある。したがって、暗号化コンテンツデータの複製が自由に行なわれても、暗号化コンテンツデータの著作者の著作権は保護されている。

【0016】

【発明が解決しようとする課題】しかし、暗号化コンテンツデータをプレゼントされたユーザが、そのプレゼントされた／複製した暗号化コンテンツデータを復号および再生した後に、もう必要がないと思ってプレゼントされた暗号化コンテンツデータをメモリカードから削除することがある。そして、削除した後に、再度、以前にプレゼントされた／複製した暗号化コンテンツデータが必要になることがある。このような場合、暗号化コンテンツデータを配信サーバから受信するのでは、配信サーバとの通信時間が長くなり、手続きも煩雑であるという問題がある。

【0017】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、複製されたコンテンツデータを受信したデータ端末装置が以前に受信したコンテンツデータを容易に再取得できるデータ端末装置およびデータ再取得方法を提供することである。

【0018】

【課題を解決するための手段】この発明によれば、データ端末装置は、複製されたコンテンツデータとコンテンツデータの付加情報とコンテンツデータの複製元の固有情報とを含むデータを受信し、複製元に関する情報を管理するデータ端末装置であって、コンテンツデータを記録するデータ記録装置との間でデータのやり取りを行なうインタフェースと、外部とのデータのやり取りを行なう送受信手段と、複製元に関する情報を管理する情報管理手段と、データからコンテンツデータと固有情報と付加情報とを取得する取得手段と、制御手段とを備え、制御手段は、送受信手段を介してデータを受信すると、その受信したデータを取得手段に与え、取得手段により取得されたコンテンツデータをインタフェースを介してデータ記録装置に記録し、取得手段により取得された固有情報と付加情報とを複製元に関する情報として情報管理手段に格納する。

【0019】したがって、この発明によれば、複製先のデータ端末装置は、コンテンツデータの複製により複製元の固有情報を取得できる。

【0020】また、この発明によれば、データ端末装置

は、複製されたコンテンツデータおよびコンテンツデータの付加情報を含むデータと、コンテンツデータの複製元にアクセスするアクセス情報とを受信し、複製元に関する情報を管理するデータ端末装置であって、コンテンツデータを記録するデータ記録装置との間でデータのやり取りを行なうインタフェースと、外部とのデータのやり取りを行なう送受信手段と、複製元に関する情報を管理する情報管理手段と、複製元の固有情報を生成する情報生成手段と、データから前記コンテンツデータと付加情報とを取得する取得手段と、制御手段とを備え、制御手段は、送受信手段を介してデータを受信すると、その受信したデータを取得手段に与え、送受信手段を介して受信したアクセス情報を情報生成手段に与え、取得手段により取得されたコンテンツデータをインタフェースを介してデータ記録装置に記録し、情報生成手段によって生成された固有情報と取得手段により取得された付加情報とを複製元に関する情報として情報管理手段に格納し、情報生成手段は、与えられたアクセス情報を用いて固有情報を生成し、その生成した固有情報を制御手段に与える。

【0021】したがって、この発明によれば、複製先のデータ端末装置は、複製元の固有情報を自ら生成できる。

【0022】好ましくは、データ端末装置は、指示を入力するためのキー操作手段と、各種の情報を視覚情報としてユーザに表示する表示手段とをさらに備え、制御手段は、キー操作手段を介して入力された複製元に関する情報の表示要求に応じて、情報管理手段から複製元に関する情報を読み出して表示手段に与え、表示手段によって表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求がキー操作手段を介して入力されると、固有情報に含まれるアクセス情報を用いて複製元のデータ端末装置からコンテンツデータを再取得し、表示手段は、複製元に対応する情報を表示する。

【0023】したがって、この発明によれば、ユーザは、自己のデータ端末装置の表示画面において複製したいコンテンツデータを選択するだけでコンテンツデータを自動的に複製できる。

【0024】好ましくは、データ端末装置は、指示を入力するためのキー操作手段と、各種の情報を視覚情報としてユーザに表示する表示手段とをさらに備え、情報管理手段は、複製元のデータ端末装置から受信したコンテンツデータの個数に応じた複数の複製元に関する情報を管理し、制御手段は、キー操作手段を介して入力された複製元に関する情報の表示要求に応じて、情報管理手段から複数の複製元に関する情報を読み出して表示手段に与え、表示手段によって表示された複数の複製元に関する情報のうちユーザによって選択された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再

取得要求がキー操作手段を介して入力されると、固有情報に含まれるアクセス情報を用いて選択されたコンテンツデータの複製元のデータ端末装置からコンテンツデータを再取得し、表示手段は、複数の複製元に対応する情報を表示する。

【0025】したがって、この発明によれば、ユーザは、以前に複製した複数のコンテンツデータから、再度、複製したいコンテンツデータを選択し、かつ、その選択したコンテンツデータを自動的に複製できる。

【0026】好ましくは、制御手段は、複製元のデータ端末装置がコンテンツデータの複製に応じたとき、送受信手段を介して複製元のデータ端末装置からコンテンツデータを再取得する。

【0027】したがって、この発明によれば、コンテンツデータの不正な複製を防止できる。

【0028】好ましくは、コンテンツデータは、ライセンス鍵によって暗号化された暗号化コンテンツデータであり、制御手段は、キー操作手段を介して入力されたライセンス鍵を含むライセンスの配信要求に応じて、ライセンスを保持するサーバへアクセスし、サーバからライセンスを受信する。

【0029】したがって、この発明によれば、著作権を保護しながら、コンテンツデータの複製を促進できる。

【0030】また、この発明によれば、データ再取得方法は、複製されたコンテンツデータとコンテンツデータの付加情報とコンテンツデータの複製元の固有情報とを含むデータを受信し、付加情報および固有情報をコンテンツデータの複製元に関する情報として管理するデータ端末装置においてコンテンツデータを複製元のデータ端末装置から再取得するデータ再取得方法であって、受信した複製元に関する情報を表示手段に表示する第1のステップと、表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求を受け付ける第2のステップと、表示された複製元に関する情報に含まれる固有情報に基づいて再取得要求がなされたコンテンツデータの複製元にアクセスし、複製元のデータ端末装置から複製されたコンテンツデータを再取得する第3のステップとを含む。

【0031】したがって、この発明によれば、複製元の固有情報に基づいてコンテンツデータを複製元から容易に再取得できる。

【0032】また、この発明によれば、データ再取得方法は、複製されたコンテンツデータおよびコンテンツデータの付加情報を含むデータと、コンテンツデータの複製元にアクセスするアクセス情報とを受信し、付加情報と受信したアクセス情報を用いて生成された前記複製元の固有情報とを前記複製元に関する情報として管理するデータ端末装置においてコンテンツデータを複製元のデータ端末装置から再取得するデータ再取得方法であって、受信した複製元に関する情報を表示手段に表示する

第1のステップと、表示された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求を受付ける第2のステップと、表示された複製元に関する情報に含まれる固有情報に基づいて再取得要求がなされたコンテンツデータの複製元にアクセスし、複製元のデータ端末装置から複製されたコンテンツデータを再取得する第3のステップとを含む。

【0033】したがって、この発明によれば、複製元の固有情報として複製元のアクセス情報のみを受信する場合においても、複製元の固有情報に基づいてコンテンツデータを複製元から容易に再取得できる。

【0034】好ましくは、第1のステップにおいて、複製元のデータ端末装置から受信したコンテンツデータの個数に応じた複数の複製元に関する情報を表示し、第2のステップにおいて、表示された複数の複製元に関する情報のうちユーザによって選択された複製元に関する情報に含まれる付加情報に対応するコンテンツデータの再取得要求が受け付けられる。

【0035】したがって、この発明によれば、以前の複製した複数のコンテンツデータから、再度、複製したいコンテンツデータを選択し、かつ、その選択したコンテンツデータを自動的に再複製できる。

【0036】好ましくは、第3のステップにおいて、複製元のデータ端末装置がコンテンツデータの複製を許可したとき、複製元のデータ端末装置からコンテンツデータを再取得する。

【0037】したがって、この発明によれば、コンテンツデータの不正な複製を防止できる。

【0038】好ましくは、コンテンツデータは、ライセンス鍵によって暗号化された暗号化コンテンツデータであり、ライセンス鍵を含むライセンスの配信要求を受付ける第4のステップと、ライセンスを保持するサーバへアクセスし、サーバからライセンスを受信する第5のステップとをさらに含む。

【0039】したがって、この発明によれば、著作権を保護しながら、コンテンツデータの複製を促進できる。

【0040】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0041】図1は、本発明の実施の形態によるデータ端末装置へ暗号化コンテンツデータを配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0042】なお、以下では携帯電話網を介してデジタル音楽データをユーザの携帯電話機100、102、104、106に装着されたメモリカード110、112、114、116に配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることな

く、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【0043】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ10に中継する。著作権の存在する音楽データを管理する配信サーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100、102、104、106に装着されたメモリカード110、112、114、116が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを与える。

【0044】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100、102、104、106に装着されたメモリカード110、112、114、116に対して、携帯電話網および携帯電話機100、102、104、106を介して暗号化コンテンツデータとライセンスとを配信する。

【0045】図1においては、たとえば携帯電話ユーザの携帯電話機100、102、104、106には、それぞれ、着脱可能なメモリカード110、112、114、116が装着される構成となっている。メモリカード110、112、114、116は、それぞれ、携帯電話機100、102、104、106により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機100、102、104、106中の音楽再生部（図示せず）に与える。

【0046】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。図1においては、携帯電話機102、104、106へのヘッドホンの接続を省略してあるが、携帯電話機102、104、106においてもヘッドホンを介して再生したコンテンツデータを聴取できる。

【0047】このような構成とすることで、まず、メモリカード110、112、114、116を利用しないと、配信サーバ10からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0048】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテン

データを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0049】また、図1においては、配信サーバ10から配信キャリア20を介して携帯電話機100、102、104、106へ配信された暗号化コンテンツデータの複製が、複数の携帯電話機100、102、104、106の間で行なわれ、その複製された暗号化コンテンツデータを受信した携帯電話機100（または102、104、106）は、受信した暗号化コンテンツデータを装着されたメモリカード110（または112、114、116）に格納するとともに、受信した暗号化コンテンツデータに付加された複製元の固有情報を保持する。そして、携帯電話機100（または102、104、106）は、複製された暗号化コンテンツデータを削除した場合、または受信した暗号化コンテンツデータを記録したメモリカード110（112、114、116）がない場合に、複製された暗号化コンテンツデータが必要になったとき、自己が保持する複製元の固有情報に基づいて複製元の携帯電話機からコンテンツデータを再取得する。

【0050】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機のユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータの保護を実現する構成である。

【0051】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0052】なお、以下の説明においては、配信サーバ10から、各携帯電話機にコンテンツデータを伝送する処理を「配信」と称することとする。

【0053】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0054】まず、配信サーバ10より配信されるデータについて説明する。Dcは、音楽データ等のコンテンツデータである。コンテンツデータDcは、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵K

cによって復号可能な暗号化が施された暗号化コンテンツデータ{Dc}Kcがこの形式で配信サーバ10より携帯電話機100、102、104、106のユーザに配布される。

【0055】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0056】さらに、配信サーバ10からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Dc-infが配布される。また、ライセンスとして、ライセンス鍵Kc、配信サーバ10からのライセンス鍵等の配信を特定するための管理コードであるトランザクションIDが配信サーバ10と携帯電話機100、102、104、106との間でやり取りされる。

【0057】さらに、ライセンスとしては、コンテンツデータDcを識別するためのコードであるコンテンツIDや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置（メモリカード）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ACmおよびデータ再生端末における再生に関する制御情報である再生制御情報ACp等が存在する。具体的には、アクセス制御情報ACmはメモリカードからライセンスまたはライセンス鍵を外部に出力するに当たっての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する回数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ACpは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【0058】以後、トランザクションIDとコンテンツIDとを併せてライセンスIDと総称し、ライセンス鍵KcとライセンスIDとアクセス制御情報ACmと再生制御情報ACpとを併せて、ライセンスと総称することとする。

【0059】また、以降では、簡単化のためアクセス制御情報ACmは再生回数の制限を行なう制御情報である再生回数（0：再生不可、1～254：再生可能回数、255：制限無し）、ライセンスの移動および複製を制限する移動・複製フラグ（0：移動複製禁止、1：移動のみ可、2：移動複製可）の2項目とし、再生制御情報ACpは再生可能な期限を規定する制御情報である再生期限（UTCtimeコード）のみを制限するものとする。

【0060】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および



再生を禁止することができるように禁止クラスリストCRL(Class Revocation List)の運用を行なう。以下では、必要に応じて記号CRLによって禁止クラスリスト内のデータを表わすこともある。

【0061】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機、およびメモ리카ードのクラスをリストアップした禁止クラスリストデータCRLが含まれる。コンテンツデータの保護にかかわるライセンスの管理・蓄積および再生を行なう全ての機器およびプログラムがリストアップの対象となる。

【0062】禁止クラスリストデータCRLは、配信サーバ10内で管理されるとともに、メモ리카ード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび／またはライセンス鍵等のライセンスを配信する際に、携帯電話機から受取った禁止クラスリストの更新日時を判断し、所有する禁止クラスリストCRLの更新日時と比較して更新されていないと判断されたとき、更新された禁止クラスリストを携帯電話機に配信する。また、禁止クラスリストの変更については、変更点のみを反映した差分データである差分CRLを配信サーバ10側より発生して、これに応じてメモ리카ード内の禁止クラスリストCRLに追加する構成とすることも可能である。また、メモ리카ード内で管理される禁止クラスリストCRLには更新日時CRLdateも更新時に記録されているものとする。

【0063】このように、禁止クラスリストCRLを、配信サーバのみならずライセンスを記録して管理するメモ리카ードにおいても保持運用することによって、再生やライセンスの移動・複製などに際して、クラス固有すなわち、コンテンツ再生回路(携帯電話機および再生端末)の種類に固有の復号鍵が破られた、コンテンツ再生回路(携帯電話機および再生端末)へのライセンス鍵あるいはライセンスの供給を禁止する。このため、携帯電話機ではコンテンツデータの再生が、メモ리카ードではライセンスの取得が行なえなくなり、新たなコンテンツデータを受信することができなくなる。

【0064】このように、メモ리카ード内の禁止クラスリストCRLは配信時に逐次データを更新する構成とする。また、メモ리카ード内における禁止クラスリストCRLの管理は、上位レベルとは独立にメモ리카ード内では、ハード的に機密性を保証する高いレベルの耐タンパモジュール(Tamper Resistant Module)に記録する。

【0065】図3は、図1に示すデータ配信システムにおいて使用される通信のためのデータ、情報等の特性を説明する図である。

【0066】コンテンツ再生回路、およびメモ리카ードには固有の公開暗号鍵K P p yおよびK P m wがそれぞれ設けられ、公開暗号鍵K P p yおよびK P m wはコンテンツ再生回路に固有の秘密復号鍵K p yおよびメモ리카ードに固有の秘密復号鍵K m wによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、コンテンツ再生デバイス、およびメモ리카ードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【0067】また、コンテンツ再生回路(携帯電話機、再生端末)のクラス証明書としてC p yが設けられ、メモ리카ードのクラス証明書としてC m wが設けられる。これらのクラス証明書は、コンテンツ再生回路、およびメモ리카ードのクラスごとに異なる情報を有する。耐タンパモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、秘密復号鍵が漏洩したクラスに対しては、禁止クラスリストにリストアップされてライセンス取得の禁止対象となる。

【0068】これらのコンテンツ再生回路のクラス公開暗号鍵およびクラス証明書は、認証データ{K P p y / C p y} K P aの形式で、メモ리카ードのクラス公開暗号鍵およびクラス証明書は認証データ{K P m w / C m w} K P aの形式で、出荷時にデータ再生回路、およびメモ리카ードにそれぞれ記録される。後ほど詳細に説明するが、K P aは配信システム全体で共通の公開認証鍵である。

【0069】また、メモ리카ード110, 112, 114, 116内のデータ処理を管理するための鍵として、メモ리카ードという媒体ごとに設定される公開暗号鍵K P m c xと、公開暗号鍵K P m c xで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵K m c xが存在する。このメモ리카ードごとに個別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵K P m c xを個別公開暗号鍵、秘密復号鍵K m c xを個別秘密復号鍵と称する。

【0070】メモ리카ード外とメモ리카ード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ10、携帯電話機100, 102, 104, 106、メモ리카ード110, 112, 114, 116において生成される共通鍵K s 1~K s 3が用いられる。

【0071】ここで、共通鍵K s 1~K s 3は、配信サーバ、コンテンツ再生回路もしくはメモ리카ード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵K s 1~K s 3を「セッションキー」とも呼ぶこととする。

【0072】これらのセッションキーKs1～Ks3は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生回路、およびメモリカードによって管理される。具体的には、セッションキーKs1は、配信サーバによって配信セッションごとに発生される。セッションキーKs2は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーKs3は、コンテンツ再生回路において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0073】図4は、図1に示した配信サーバ10の構成を示す概略ブロック図である。配信サーバ10は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツID等の配信情報を保持するための情報データベース304と、携帯電話機の各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、禁止クラスリストCRLを管理するCRLデータベース306と、情報データベース304に保持されたコンテンツデータのメニューを保持するメニューデータベース307と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションID等の配信に関するログを保持する配信記録データベース308と、情報データベース304、課金データベース302、CRLデータベース306、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0074】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモリカードから送られてきた認証のための認証データ {K Pmw / Cmw} KPaを復号するための公開認証鍵KPaを保持する認証鍵保持部313と、メモリカードから送られてきた認証のための認証データ {K Pmw / Cmw} KPaを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵KPaによって復号処理を行なう復号処理部312と、配信セッションごとに、セッション鍵Ks1を発生するセッションキー発生部316、セッションキー発生部316より生成されたセッションキーKs1を復号処理部312によって得られたクラス公開暗号鍵K Pmwを用いて暗号

化して、バスBS1に出力するための暗号化処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号処理を行なう復号処理部320とを含む。

【0075】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよびアクセス制御情報ACmを、復号処理部320によって得られたメモリカードごとに固有の公開暗号鍵K Pmc xによって暗号化するための暗号化処理部326と、暗号化処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号化処理部328とを含む。

【0076】配信サーバ10の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0077】図5は、図1に示した携帯電話機100、102、104、106の構成を説明するための概略ブロック図である。

【0078】携帯電話機100、102、104、106は、携帯電話網により無線伝送される信号を受信するアンテナ1100と、アンテナ1100からの信号を受けてベースバンド信号に変換、あるいは携帯電話機100、102、104、106からのデータを変調してアンテナ1100に与える送受信部1102と、携帯電話機100、102、104、106の各部のデータ授受を行なうバスBS2とを含む。

【0079】携帯電話機100、102、104、106は、さらに、携帯電話機100、102、104、106のユーザの音声データを取込み、音声データをAD変換部1106へ出力するマイク1104と、音声データをアナログ信号からデジタル信号に変換するAD変換部1106と、デジタル信号に変換された音声信号を所定の方式に符号化する音声符号化部1108とを含む。

【0080】携帯電話機100、102、104、106は、さらに、他の携帯電話機から受信した音声信号を復号する音声再生部1110と、音声再生部1110からの音声信号をデジタル信号からアナログ信号に変換して音声データを出力するDA変換部1112と、音声データを外部へ出力するスピーカ1114とを含む。

【0081】携帯電話機100、102、104、106は、さらに、外部からの指示を携帯電話機100、102、104、106に与えるための操作パネル1116と、コントローラ1120等から出力される情報をユーザに視覚情報として与えるための表示パネル1118と、情報取得部1121により取得された暗号化コンテンツデータの付加情報および複製元の個人情報を記憶するメモリ1119と、バスBS2を介して携帯電話機100、102、104、106の動作を制御するためのコントローラ1120と、複製された暗号化コンテンツデータを受信した際に、その受信した暗号化コンテンツ

データに付加された付加情報および複製元の個人情報を取得する情報取得部1121とを含む。

【0082】携帯電話機100、102、104、106は、さらに、配信サーバ10からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード110、112、114、116と、メモリカード110、112、114、116とバスBS2との間のデータの授受を制御するためのメモリカードインタフェース1200とを含む。

【0083】携帯電話機100、102、104、106は、さらに、クラス公開暗号鍵K P p 1およびクラス証明書C p 1を公開認証鍵K P aで復号することでその正当性を認証できる状態に暗号化した認証データ {K P p 1 / C p 1} K P aを保持する認証データ保持部1500を含む。ここで、携帯電話機100のクラスyは、y=1であるとする。

【0084】携帯電話機100、102、104、106は、さらに、クラス固有の復号鍵であるK p 1を保持するK p 1保持部1502と、バスBS2から受けたデータをK p 1によって復号し、メモリカード110、112、114、116によって発生されたセッションキーK s 2を得る復号処理部1504とを含む。

【0085】携帯電話機100、102、104、106は、さらに、メモリカード110、112、114、116に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110、112、114、116との間でバスBS2上においてやり取りされるデータを暗号化するためのセッションキーK s 3を乱数等により発生するセッションキー発生部1508と、暗号化コンテンツデータの再生セッションにおいてメモリカード110、112、114、116からライセンス鍵K cおよび再生制御情報A C pを受取る際に、セッションキー発生部1508により発生されたセッションキーK s 3を復号処理部1504によって得られたセッションキーK s 2によって暗号化し、バスBS3に出力する暗号化処理部1506とを含む。

【0086】携帯電話機100、102、104、106は、さらに、バスBS2上のデータをセッションキーK s 3によって復号して、ライセンス鍵K cおよび再生制御情報A C pを出力する復号処理部1510と、バスBS2より暗号化コンテンツデータ {D c} K cを受けて、復号処理部1510より取得したライセンス鍵K cによって復号し、コンテンツデータを出力する復号処理部1516と、復号処理部1516の出力を受けてコンテンツデータを再生するための音楽再生部1518と、音楽再生部1518の出力をデジタル信号からアナログ信号に変換するDA変換器1519と、DA変換器1519の出力をヘッドホンなどの外部出力装置（図示省略）へ出力するための端子1530とを含む。

【0087】なお、図5においては、点線で囲んだ領域

は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス1550を構成する。

【0088】携帯電話機100、102、104、106の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0089】図6は、図1に示すメモリカード110の構成を説明するための概略ブロック図である。

【0090】既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、K P m wおよびK m wが設けられ、メモリカードのクラス証明書C m wが設けられるが、メモリカード110においては、自然数w=3で表わされるものとする。また、メモリカードを識別する自然数xはx=4で表されるものとする。

【0091】したがって、メモリカード110は、認証データ {K P m 3 / C m 3} K P aを保持する認証データ保持部1400と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵K m c 4を保持するK m c 保持部1402と、クラス秘密復号鍵K m 3を保持するK m 保持部1421と、個別秘密復号鍵K m c 4によって復号可能な公開暗号鍵K P m c 4を保持するK P m c 保持部1416とを含む。

【0092】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0093】メモリカード110は、さらに、メモリインタフェース1200との間で信号を端子1426を介して授受するインタフェース1424と、インタフェース1424との間で信号をやり取りするバスBS3と、バスBS3にインタフェース1424から与えられるデータから、クラス秘密復号鍵K m 3をK m 保持部1421から受けて、配信サーバ10が配信セッションにおいて生成したセッションキーK s 1を接点P aに出力する復号処理部1422と、K P a保持部1414から公開認証鍵K P aを受けて、バスBS3に与えられるデータから公開認証鍵K P aによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ1420に、得られたクラス公開鍵を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1446によって選択的に与えられるデータを暗号化してバスBS3に出力する暗号化処理部1406とを含む。

【0094】メモリカード110は、さらに、配信、および再生の各セッションにおいてセッションキーK s 2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーK s 2を復号処理部1408によって得られるクラス公開暗号鍵K P p yもしくはK P m wによって暗号化してバスB

S3に送出する暗号化処理部1410と、バスBS4よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号する復号処理部1412と、暗号化コンテンツデータの再生セッションにおいてメモリ1415から読出されたライセンス鍵Kcおよび再生制御情報ACpを、復号処理部1412で復号された他のメモリカード110の個別公開暗号鍵Kpmcx(≠4)で暗号化する暗号処理部1417とを含む。

【0095】メモリカード110は、さらに、バスBS3上のデータを個別公開暗号鍵Kpmc4と対をなすメモリカード110の個別秘密復号鍵Kmc4によって復号するための復号処理部1404と、禁止クラスリストのバージョン更新のためのデータCRL\_datによって逐次更新される禁止クラスリストデータCRLと、暗号化コンテンツデータ{Dc}Kcと、暗号化コンテンツデータ{Dc}Kcを再生するためのライセンス(Kc, ACp, ACm, ライセンスID)と、付加情報Data-infと、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバスBS3より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモリによって構成される。また、メモリ1515は、CRL領域1415Aと、ライセンス領域1415Bと、データ領域1415Cとから成る。CRL領域1415Aは、禁止クラスリストCRLを記録するための領域である。ライセンス領域1415Bは、ライセンスを記録するための領域である。データ領域1415Cは、暗号化コンテンツデータ{Dc}Kc、暗号化コンテンツデータの関連情報Dc-inf、ライセンスを管理するために必要な情報を暗号化コンテンツごとに記録するライセンス管理ファイル、およびメモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リストファイルを記録するための領域である。そして、データ領域1415Cは、外部から直接アクセスが可能である。ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【0096】ライセンス領域1415Bは、ライセンス(ライセンス鍵Kc、再生制御情報ACp、アクセス制限情報ACm、ライセンスID)を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスを格納する。ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【0097】メモリカード110は、さらに、バスBS3を介して外部との間でデータ授受を行ない、バスBS3との間で再生情報等を受けて、メモリカード110の動作を制御するためのコントローラ1420を含む。

【0098】なお、データ領域1415Cを除く全ての構成は、耐タンパモジュール領域に構成される。

【0099】メモリカード112, 114, 116は、メモリカード110と同じ構成から成る。この場合、メモリカード112, 114, 116においては、自然数wは3以外の自然数が設定され、自然数xは4以外の自然数が設定される。

【0100】以下、図1に示すデータ配信システムにおける各セッションの動作について説明する。

【0101】[配信1] まず、図1に示すデータ配信システムにおいて、配信サーバ10から携帯電話機100に装着されたメモリカード110へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。なお、この動作を「配信」という。

【0102】図7～図10は、図1に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する携帯電話機100に装着されたメモリカード110への配信動作(以下、配信セッションともいう)を説明するための第1～第4のフローチャートである。

【0103】図7における処理以前に、携帯電話機100のユーザは、配信サーバ10に対して接続し、購入を希望するコンテンツに対するコンテンツIDを取得していることを前提としている。

【0104】図7を参照して、携帯電話機100のユーザから操作パネル1116を介してコンテンツIDの指定による配信リクエストがなされる(ステップS100)。そして、操作パネル1116を介して暗号化コンテンツデータのライセンスを購入するための購入条件ACが入力される(ステップS102)。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Kcを購入するために、暗号化コンテンツデータのアクセス制御情報ACm、および再生制御情報ACpを設定して購入条件ACが入力される。

【0105】暗号化コンテンツデータの購入条件ACが入力されると、コントローラ1120は、バスBS2およびメモリカードインタフェース1200を介してメモリカード110へ認証データの出力指示を与える(ステップS104)。メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS3を介して認証データの出力指示を受取る。そして、コントローラ1420は、バスBS3を介して認証データ保持部1400から認証データ{Kpm3/Cm3}KPaを読み出し、{Kpm3/Cm3}KPaをバスBS3、インタフェース1424および端子1426を介して出力する(ステップS106)。

【0106】携帯電話機100のコントローラ1120は、メモリカード110からの認証データ{Kpm3/Cm3}KPaに加えて、コンテンツID、ライセンス購入条件のデータAC、および配信リクエストを配信サーバ10に対して送信する(ステップS108)。

【0107】配信サーバ10では、携帯電話機100から配信リクエスト、コンテンツID、認証データ{K P m 3 / / C m 3} K P a、およびライセンス購入条件のデータACを受信し(ステップS110)、復号処理部312においてメモリカード110から出力された認証データを公開認証鍵K P aで復号処理を実行する(ステップS112)。

【0108】配信制御部315は、復号処理部312における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS114)。正当な認証データであると判断された場合、配信制御部315は、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を承認し、受理する。そして、次の処理(ステップS116)へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を受理しないで配信セッションを終了する(ステップS198)。

【0109】認証の結果、クラス公開暗号鍵K P m 3およびクラス証明書C m 3を受理すると、配信制御部315は、次に、メモリカード110のクラス証明書C m 3が禁止クラスリストC R LにリストアップされているかどうかをC R Lデータベース306に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する(ステップS198)。

【0110】一方、メモリカード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS116)。

【0111】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ10において、配信制御部315は、配信を特定するための管理コードであるトランザクションIDを生成する(ステップS118)。また、セッションキー発生部316は、配信のためのセッションキーK s 1を生成する(ステップS120)。セッションキーK s 1は、復号処理部312によって得られたメモリカード110に対応するクラス公開暗号鍵K P m 3によって、暗号化処理部318によって暗号化される(ステップS122)。

【0112】トランザクションIDおよび暗号化されたセッションキーK s 1は、トランザクションID / / {K s 1} K m 3として、バスB S 1および通信装置350を介して外部に出力される(ステップS124)。

【0113】図8を参照して、携帯電話機100が、トランザクションID / / {K s 1} K m 3を受信すると(ステップS126)、コントローラ1120は、トランザクションID / / {K s 1} K m 3をメモリカード110に入力する(ステップS128)。そうすると、

メモリカード110においては、端子1426およびインタフェース1424を介して、バスB S 3に与えられた受信データを、復号処理部1422が、保持部1421に保持されるメモリカード110に固有なクラス秘密復号鍵K m 3によって復号処理することにより、セッションキーK s 1を復号し、セッションキーK s 1を受理する(ステップS130)。

【0114】コントローラ1420は、配信サーバ10で生成されたセッションキーK s 1の受理を確認すると、セッションキー発生部1418に対してメモリカード110において配信動作時に生成されるセッションキーK s 2の生成を指示する。そして、セッションキー発生部1418は、セッションキーK s 2を生成する(ステップS132)。

【0115】また、配信セッションにおいては、コントローラ1420は、メモリカード110内のメモリ1415に記録されている禁止クラスリストC R Lから更新日時C R L d a t eを抽出して切換スイッチ1446に出力する(ステップS134)。

【0116】暗号処理部1406は、切換スイッチ1442の接点P aを介して復号処理部1422より与えられるセッションキーK s 1によって、切換スイッチ1446の接点を順次切換えることによって与えられるセッションキーK s 2、個別公開暗号鍵K P m c 4および禁止クラスリストの更新日時C R L d a t eを1つのデータ列として暗号化して、{K s 2 / / K P m c 4 / / C R L d a t e} K s 1をバスB S 3に出力する(ステップS136)。

【0117】バスB S 3に出力された暗号化データ{K s 2 / / K P m c 4 / / C R L d a t e} K s 1は、バスB S 3からインタフェース1424および端子1426を介して携帯電話機100に出力され、携帯電話機100から配信サーバ10に送信される(ステップS138)。

【0118】配信サーバ10は、トランザクションID / / {K s 2 / / K P m c 4 / / C R L d a t e} K s 1を受信して、復号処理部320においてセッションキーK s 1による復号処理を実行し、メモリカード110で生成されたセッションキーK s 2、メモリカード110に固有の公開暗号鍵K P m c 4およびメモリカード110における禁止クラスリストC R Lの更新日時C R L d a t eを受理する(ステップS142)。

【0119】配信制御部315は、ステップS110で取得したコンテンツIDおよびライセンス購入条件のデータACに従って、アクセス制御情報A C mおよび再生制御情報A C pを生成する(ステップS144)。さらに、暗号化コンテンツデータを復号するためのライセンス鍵K cを情報データベース304より取得する(ステップS146)。

【0120】配信制御部315は、生成したライセン

ス、すなわち、トランザクションID、コンテンツID、ライセンス鍵Kc、再生制御情報ACp、およびアクセス制御情報ACmを暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたメモリカード110に固有の公開暗号鍵Kpmc4によってライセンスを暗号化して暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4を生成する(ステップS148)。

【0121】図9を参照して、配信サーバ10において、メモリカード110から送信された禁止クラスリストの更新日時CRLdateが、CRLデータベース306に保持される配信サーバ10の禁止クラスリストCRLの更新日時と比較されることによってメモリカード110が保持する禁止クラスリストCRLが最新か否かが判断され、メモリカード110が保持する禁止クラスリストCRLが最新と判断されたとき、ステップS152へ移行する。また、メモリカード110が保持する禁止クラスリストCRLが最新でないときはステップS160へ移行する(ステップS150)。

【0122】最新と判断されたとき、暗号化処理部328は、暗号化処理部326から出力された暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4をメモリカード110において発生されたセッションキーKs2によって暗号化を行ない、暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2をバスBS1に出力する。そして、配信制御部315は、バスBS1上の暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を通信装置350を介して携帯電話機100へ送信する(ステップS152)。

【0123】そして、携帯電話機100のコントローラ1120は、暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を受信し(ステップS154)、バスBS2およびメモリカードインタフェース1200を介してメモリカード110に入力する。メモリカード110の復号処理部1412は、暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を端子1426およびインタフェース1424を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2によって復号し、{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4を受信する(ステップS158)。その後、ステップS172へ移行する。

【0124】一方、配信サーバ10において、メモリカード110が保持する禁止クラスリストCRLが最新でないと判断されると、配信制御部315は、バスBS1

を介してCRLデータベース306から最新の禁止クラスリストCRLを取得し、差分データである差分CRLを生成する(ステップS160)。

【0125】暗号化処理部328は、暗号化処理部326の出力と、配信制御部315がバスBS1を介して供給する禁止クラスリストの差分CRLとを受けて、メモリカード110において生成されたセッションキーKs2によって暗号化する。暗号化処理部328より出力された暗号化データ{差分CRL//トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2は、バスBS1および通信装置350を介して携帯電話機100に送信される(ステップS162)。

【0126】携帯電話機100は、送信された暗号化データ{差分CRL//トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を受信し(ステップS164)、バスBS2およびメモリカードインタフェース1200を介してメモリカード110に入力する(ステップS166)。メモリカード110においては、端子1426およびインタフェース1424を介して、バスBS3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS3上の受信データを復号しバスBS3に出力する(ステップS168)。

【0127】この段階で、バスBS3には、Kmc保持部1402に保持される秘密復号鍵Kmc4で復号可能な暗号化ライセンス{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4と、差分CRLとが出力される(ステップS168)。コントローラ1420の指示によって受理した差分CRLによってメモリ1415内のCRL領域1415Aを差分CRLに基づいて更新する(ステップS170)。

【0128】ステップS152、S154、S156、S158は、メモリカード110の禁止クラスリストCRLが最新の場合のライセンスのメモリカード110への配信動作であり、ステップS160、S162、S164、S166、S168、S170は、メモリカード110の禁止クラスリストCRLが最新でない場合のライセンスのメモリカード110への配信動作である。このように、メモリカード110から送られてきた禁止クラスリストの更新日時CRLdateによって、配信を求めてきたメモリカード110の禁止クラスリストCRLが最新か否かを、逐一、確認し、最新でないとき、最新の禁止クラスリストCRLをCRLデータベース306から取得し、差分CRLをメモリカード110に配信することによって、ライセンスの破られたメモリカードへのライセンスの配信を防止できる。

【0129】ステップS158またはステップS170

の後、コントローラ1420の指示によって、暗号化ライセンス {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4は、復号処理部1404において、個別秘密復号鍵Kmc4によって復号され、ライセンス (ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp) が受理される (ステップS172)。

【0130】図10を参照して、携帯電話機100のコントローラ1120は、メモリカード110が受理した 10 ライセンスを格納するエントリを指示するためのエントリ番号を、メモリカード110に入力する (ステップS174)。そうすると、メモリカード110のコントローラ1420は、端子1426およびインタフェース1424を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ1415のライセンス領域1415Bに、ステップS172において取得したライセンス (ライセンス鍵Kc、トランザクションID、コンテンツID、アクセス制御情報ACmおよび再生制御情報ACp) を格納する (ステップS176)。

【0131】そして、携帯電話機100のコントローラ1120は、配信サーバ10から送られたトランザクションIDと、暗号化コンテンツデータの配信要求を配信サーバ10へ送信する (ステップS178)。

【0132】配信サーバ10は、トランザクションIDおよび暗号化コンテンツデータの配信要求を受信し (ステップS180)、情報データベース304より、暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-i n fを取得して、これらのデータをバスBS1および 20 通信装置350を介して出力する (ステップS182)。

【0133】携帯電話機100は、{Dc} Kc//Dc-i n fを受信して、暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-i n fを受理する (ステップS184)。そうすると、携帯電話機100のコントローラ1120は、暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-i n fを1つのコンテンツファイルとしてバスBS2およびメモリカードインタフェース1200を介してメモリカード110へ入力する 40 (ステップS186)。

【0134】そうすると、メモリカード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS3を介して暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-i n fを受取り、その受取った暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-i n fをバスBS3を介してメモリ1415のデータ領域1415Cに記録する (ステップS187)。また、コントローラ1420は、メモリカード110に格納されたライセンスのエントリ番号と、平 50

文のトランザクションIDおよびコンテンツIDを含む暗号化コンテンツデータ {Dc} Kcと付加情報Dc-i n fに対するライセンス管理ファイルを生成し、バスBS3を介してメモリ1415のデータ領域1415Cに記録する (ステップS188)。さらに、コントローラ1420は、メモリ1415に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Dc-i n fから抽出した暗号化コンテンツデータに関する情報 (曲名、アーティスト名) 等を追記する (ステップS190)。そして、携帯電話機100のコントローラ1120は、トランザクションIDと配信受取を配信サーバ10へ送信する (ステップS192)。

【0135】配信サーバ10は、トランザクションID//配信受取を受信すると (ステップS194)、課金データベース302への課金データの格納、およびトランザクションIDの配信記録データベース308への記録が行われて配信終了の処理が実行され (ステップS196)、全体の処理が終了する (ステップS198)。

【0136】このようにして、携帯電話機100に装着されたメモリカード110が正規の認証データを保持する機器であること、同時に、クラス証明書Cm3とともに暗号化して送信できた公開暗号鍵Kpm3が有効であることを確認した上で、クラス証明書Cm3が禁止クラスリスト、すなわち、公開暗号鍵Kpm3による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0137】携帯電話機102に装着されたメモリカード112、携帯電話機104に装着されたメモリカード114、および携帯電話機106に装着されたメモリカード116への暗号化コンテンツデータの配信動作も図7〜図10に示すフローチャートに従って行なわれる。

【0138】[再生] 次に、図11および図12を参照してメモリカード110に記録されたコンテンツデータの携帯電話機100における再生動作について説明する。なお、図11における処理以前に、携帯電話機100のユーザは、メモリカード110のデータ領域1415Cに記録されている再生リストに従って、再生するコンテンツ (楽曲) を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【0139】図11を参照して、再生動作の開始とともに、携帯電話機100のユーザから操作パネル1116を介して再生指示が携帯電話機100にインプットされる (ステップS700)。そうすると、コントローラ1120は、バスBS2を介して認証データ保持部150

0から認証データ {K P p 1 / / C p 1} K P aを読み出し、メモリカードインタフェース1200を介してメモリカード110へ認証データ {K P p 1 / / C p 1} K P aを出力する(ステップS702)。

【0140】そうすると、メモリカード110は、認証データ {K P p 1 / / C p 1} K P aを受理する(ステップS704)。そして、メモリカード110の復号処理部1408は、受理した認証データ {K P p 1 / / C p 1} K P aを、K P a保持部1414に保持された公開認証鍵K P aによって復号し(ステップS706)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ {K P p 1 / / C p 1} K P aが正規の認証データであるか否かを判断する認証処理を行なう(ステップS708)。復号できなかった場合、ステップS748へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ1420は、取得した証明書C m 1がメモリ1415のC R L領域1415 Aから読み出した禁止クラスリストC R Lに含まれるか否かを判断する

(ステップS710)。この場合、クラス証明書C p 1には識別番号が付与されており、コントローラ1420は、受理したクラス証明書C p 1の識別番号が禁止クラスリストデータの中に存在するか否かを判別する。クラス証明書C p 1が禁止クラスリストデータに含まれると判断されると、ステップS748へ移行し、再生動作は終了する。

【0141】ステップS710において、クラス証明書C p 1が禁止クラスリストデータC R Lに含まれていないと判断されると、メモリカード110のセッションキー発生部1418は、再生セッション用のセッションキーK s 2を発生させる(ステップS712)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーK s 2を、復号処理部1408で復号された公開暗号鍵K P p 1によって暗号化した {K s 2} K p 1をバスB S 3へ出力する(ステップS714)。そうすると、コントローラ1420は、インタフェース1424および端子1426を介してメモリカードインタフェース1200へ {K s 2} K p 1を出力する(ステップS716)。携帯電話機100のコントローラ1120は、メモリカードインタフェース1200を介して {K s 2} K p 1を取得する。そして、K p 1保持部1502は、秘密復号鍵K p 1を復号処理部1504へ出力する。

【0142】復号処理部1504は、K p 1保持部1502から出力された、公開暗号鍵K P p 1と対になっている秘密復号鍵K p 1によって {K s 2} K p 1を復号し、セッションキーK s 2を暗号処理部1506へ出力する(ステップS718)。そうすると、セッションキー発生部1508は、再生セッション用のセッションキーK s 3を発生させ、セッションキーK s 3を暗号処理

部1506へ出力する(ステップS720)。暗号処理部1506は、セッションキー発生部1508からのセッションキーK s 3を復号処理部1504からのセッションキーK s 2によって暗号化して {K s 3} K s 2を出力し、コントローラ1120は、バスB S 2およびメモリカードインタフェース1200を介して {K s 3} K s 2をメモリカード110へ出力する(ステップS722)。

【0143】そうすると、メモリカード110の復号処理部1412は、端子1426、インタフェース1424、およびバスB S 3を介して {K s 3} K s 2を入力する(ステップS724)。

【0144】図12を参照して、復号処理部1412は、セッションキー発生部1418によって発生されたセッションキーK s 2によって {K s 3} K s 2を復号して、携帯電話機100で発生されたセッションキーK s 3を受理する(ステップS726)。

【0145】携帯電話機100のコントローラ1120は、メモリカード110から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し、メモリカードインタフェース1200を介してメモリカード110へ取得したエントリ番号を出力する(ステップS727)。

【0146】エントリ番号が入力に応じて、コントローラ1420は、アクセス制限情報A C mを確認する(ステップS728)。

【0147】ステップS728においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報A C mを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報A C mの再生回数を更新(1減ずる)した後に次のステップに進む(ステップS730)。一方、アクセス制限情報A C mの再生回数によって再生が制限されていない場合においては、ステップS730はスキップされ、アクセス制限情報A C mの再生回数は更新されることなく処理が次のステップ(ステップS732)に進行される。

【0148】ステップS728において、当該再生動作において再生が可能であると判断された場合には、メモリ1415のライセンス領域1415 Bに記録された再生リクエスト曲のライセンス鍵K cおよび再生制御情報A C pがバスB S 3上へ出力される(ステップS732)。

【0149】得られたライセンス鍵K cと再生制御情報A C pは、切換スイッチ1446の接点P fを介して暗号化処理部1406に送られる。暗号化処理部1406は、切換スイッチ1442の接点P bを介して復号処理部1412より受けたセッションキーK s 3によって切換スイッチ1446を介して受けたライセンス鍵K cと



再生制御情報ACpとを暗号化し、暗号化データ {Kc / / ACp} Ks3をバスBS3に出力する(ステップS734)。

【0150】バスBS3に出力された暗号化データは、インタフェース1424、端子1426、およびメモリカードインタフェース1200を介して携帯電話機100に送出される。

【0151】携帯電話機100においては、メモリカードインタフェース1200を介してバスBS2に伝達される暗号化データ {Kc / / ACp} Ks3を復号処理部1510によって復号処理を行ない、ライセンス鍵Kcおよび再生制御情報ACpを受信する(ステップS736)。復号処理部1510は、ライセンス鍵Kcを復号処理部1516に伝達し、再生制御情報ACpをバスBS2に出力する。

【0152】コントローラ1120は、バスBS2を介して、再生制御情報ACpを受信して再生の可否の確認を行なう(ステップS740)。

【0153】ステップS740においては、再生制御情報ACpによって再生不可と判断される場合には、再生動作は終了される。

【0154】ステップS740において再生可能と判断された場合、コントローラ1120は、メモリカードインタフェース1200を介してメモリカード110に暗号化コンテンツデータ {Dc} Kcを要求する。そうすると、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ {Dc} Kcを取得し、バスBS3、インタフェース1424、および端子1426を介してメモリカードインタフェース1200へ出力する(ステップS742)。

【0155】携帯電話機100のコントローラ1120は、メモリカードインタフェース1200を介して暗号化コンテンツデータ {Dc} Kcを取得し、バスBS2を介して暗号化コンテンツデータ {Dc} Kcを復号処理部1516へ与える。

【0156】そして、復号処理部1516は、暗号化コンテンツデータ {Dc} Kcを復号処理部1510から出力されたライセンス鍵Kcによって復号してコンテンツデータDcを取得する(ステップS744)。

【0157】そして、復号されたコンテンツデータDcは音楽再生部1518へ出力され、音楽再生部1518は、コンテンツデータを再生し、DA変換器1519はデジタル信号をアナログ信号に変換して端子1530へ出力する。そして、音楽データは端子1530から外部出力装置を介してヘッドホン130へ出力されて再生される(ステップS746)。これによって再生動作が終了する。

【0158】上記においては、メモリカード110に記録された暗号化コンテンツデータを携帯電話機100によって再生する場合について説明したが、メモリカード

112に記録された暗号化コンテンツデータを携帯電話機102によって再生する場合、メモリカード114に記録された暗号化コンテンツデータを携帯電話機104によって再生する場合、およびメモリカード116に記録された暗号化コンテンツデータを携帯電話機106によって再生する場合についても図11および図12に示すフローチャートに従って再生動作が行なわれる。

【0159】図13は、メモリカード110のメモリ1415におけるライセンス領域1415Bとデータ領域1415Cとを示したものである。データ領域1415Cには、再生リストファイル160とコンテンツファイル1611~161nと、ライセンス管理ファイル1621~162nとが記録されている。コンテンツファイル1611~161nは、受信した暗号化コンテンツデータ {Dc} Kcと付加情報Dc-infとを1つのファイルとして記録する。また、ライセンス管理ファイル1621~162nは、それぞれ、コンテンツファイル1611~161nに対応して記録されている。

【0160】メモリカード110は、配信サーバ10から暗号化コンテンツデータおよびライセンスを受信したとき、暗号化コンテンツデータおよびライセンスをメモリ1415に記録する。そして、ライセンスは、メモリ1415のライセンス領域1415Bのエントリ番号によって指定された領域に記録され、メモリ1415のデータ領域1415Cに記録された再生リストファイル160のライセンス管理ファイルを読出せば、エントリ番号を取得でき、その取得したエントリ番号によって対応するライセンスをライセンス領域1415Bから読出することができる。

【0161】また、ライセンス管理ファイル1622は、点線で示されているが、実際には記録されていないことを示す。コンテンツファイル1612は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、携帯電話機が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当する。

【0162】また、コンテンツファイル1613は、点線で示されているが、これは、たとえば、携帯電話機が配信サーバ10から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータだけを他の携帯電話機へ送信した場合に相当し、ライセンスはメモリ1415に存在するが暗号化コンテンツデータが存在しないことを意味する。

【0163】本発明においては、配信サーバ10から携帯電話機100、102、104、106にそれぞれ装着されたメモリカード110、112、114、116に配信された暗号化コンテンツデータは、複数の携帯電話機の間でコピー(複製)される。そして、複製元の携帯電話機100は、暗号化コンテンツデータを複製するとき、複製対象の暗号化コンテンツデータ {Dc} Kc

とその暗号化コンテンツデータ {Dc} Kcに対応する付加情報Dc-infとを装着されたメモリカード110から読出し、その読出した暗号化コンテンツデータ

{Dc} Kcに付加情報Dc-infと携帯電話機100の個人情報とを付加した複製データを作成する。そして、携帯電話機100は、複製データを複製先の携帯電話機102へ送信する。

【0164】複製先の携帯電話機102は、携帯電話機100から複製データを受信する。そして、携帯電話機102においては、複製データから暗号化コンテンツデータ {Dc} Kc、付加情報Dc-inf、および複製元の個人情報が取得され、暗号化コンテンツデータ {Dc} Kcは、携帯電話機102に装着されたメモリカード112に記録される。そして、付加情報Dc-infおよび複製元の個人情報は複製元に関する情報として携帯電話機102のメモリ1119に格納される。

【0165】携帯電話機102のユーザが受信した暗号化コンテンツデータ {Dc} Kcを再生したい場合、図7～図10に示すフローチャートに従って配信サーバ10からライセンスを受信する。そして、携帯電話機102のユーザは、複製された暗号化コンテンツデータ {Dc} Kcが不要になったとき、その暗号化コンテンツデータ {Dc} Kcを削除する。その後、携帯電話機102のユーザは、複製によって以前に受信した暗号化コンテンツデータ {Dc} Kcが必要になったとき、コンテンツデータの再取得要求を携帯電話機102にインプットする。そうすると、携帯電話機102は、メモリ1119に格納された複製元の個人情報に基づいて複製元である携帯電話機100からコンテンツデータを再取得する。

【0166】図14を参照して、暗号化コンテンツデータの複製時に、複製元である携帯電話機100において生成される複製データのデータフォーマットについて説明する。複製データ40は、ヘッダ50とエレメント51～5nとから成る。ヘッダ50は、複製対象である暗号化コンテンツデータの付加情報を主に含む。具体的には、ヘッダ50は、コンテンツID501と、コンテンツ名502と、アーティスト名503と、サイズ504と、日付505とを格納する。コンテンツID501は、複製対象である暗号化コンテンツデータを識別するための識別番号である。コンテンツ名502は、複製対象である暗号化コンテンツデータの名称である。アーティスト名503は、複製対象である暗号化コンテンツデータの著作者名である。サイズ504は、複製対象である暗号化コンテンツデータのデータサイズである。日付505は、複製を行なう日時である。

【0167】複製対象である暗号化コンテンツデータおよび携帯電話機100のユーザの個人情報は、エレメント51～5nのいずれかに格納される。たとえば、暗号化コンテンツデータは、エレメント51に格納され、個

人情報はエレメント53に格納される。なお、ヘッダ50に記載したコンテンツ名502、アーティスト名503および日付505は、エレメント51～5nのいずれか（たとえば、メタエレメント）に格納する構成としてもよい。また、コンテンツ名502、アーティスト名503および日付505は、コンテンツファイル1611～161nに記録されるため、コンテンツファイル1611～161nから取得する構成としてもよい。

【0168】複製元である携帯電話機100は、作成された複製データ40を複製先である携帯電話機102へ送信する。

【0169】図15を参照して、複製先である携帯電話機102における複製元に関する情報の管理について説明する。携帯電話機102においては、受信した複製データ40のヘッダ50からコンテンツID501、コンテンツ名502、アーティスト名503、サイズ504、および日付505が取得され、エレメント51から暗号化コンテンツデータが取得され、エレメント53から携帯電話機100のユーザの個人情報が取得される。なお、取得された暗号化コンテンツデータは、携帯電話機102に装着されたメモリカード112に記録される。

【0170】携帯電話機102のメモリ1119は、図16に示すデータベース400を保持している。データベース400は、コンテンツ番号、コンテンツ名、アーティスト名、サイズ、日付、電話番号、E-Mail、カード番号、およびその他の項目から成る。取得されたコンテンツID501、コンテンツ名502、アーティスト名503、サイズ504、および日付505は、データベース400のそれぞれコンテンツ番号、コンテンツ名、アーティスト名、サイズ、および日付の項目に格納され、取得された個人情報は、データベース400のそれぞれ電話番号、E-Mail、カード番号、およびその他の項目に格納される。なお、E-Mailは、複製元である携帯電話機100のユーザ所有する電子メールアドレス情報であり、電話番号は、携帯電話機100の電話番号であり、カード番号は、携帯電話機100のユーザが所有してクレジットカードの番号である。

【0171】このようにして、複製先の携帯電話機102においては、複製対象である暗号化コンテンツデータ {Dc} Kcの付加情報Dc-infと複製元の個人情報とから複製元に関する情報が作成され、メモリ1119に格納される。なお、データベース400は、n個の複製元に関する情報を格納可能である。

【0172】そして、携帯電話機102のユーザから複製元に関する情報の表示要求がなされると、データベース400の格納されたn個の複製元に関する情報が表示パネル1118に表示される。この場合、表示パネル1116における1つの複製元に関する情報の表示画面は、図17に示すとおりである。

【0173】図16を参照して、表示画面60は、タイ

トル名61、コンテンツID62、アーティスト名63、サイズ64、電話番号65、カード番号66、E-mail67、コピーした日時68、その他、69、再取得ボタン70、およびキャンセルボタン71から成る。タイトル名61には、データベース400から読出されたコンテンツ名に格納された内容が表示され、コンテンツID62には、データベース400から読出されたコンテンツIDが表示され、アーティスト名63には、データベース400から読出されたアーティスト名に格納された内容が表示され、サイズ64には、データベース400から読出されたサイズに格納された内容が表示され、電話番号65には、データベース400から読出された電話番号に格納された内容が表示され、カード番号66には、データベース400から読出されたカード番号に格納された内容が表示され、E-mail67には、データベース400から読出されたE-Mailに格納された内容が表示され、コピーした日時68には、データベース400から読出された日付に格納された内容が表示され、その他69には、データベース400から読出されたその他に格納された内容が表示される。

【0174】そして、携帯電話機102のユーザは、表示画面60を見て、コンテンツデータを複製元から再取得するか否かを決定する。ユーザは、コンテンツデータを再取得するとき、再取得ボタン70を押し、コンテンツデータを再取得しないとき、キャンセルボタン71を押す。なお、キャンセルボタン71を押したとき、データベース400に格納された次の複製元に関する情報が画面60のフォーマットで表示される。

【0175】複製元である携帯電話機100から複製先である携帯電話機102への暗号化コンテンツデータ {Dc} Kcの複製動作について説明する。図17は、携帯電話機100から携帯電話機102への暗号化コンテンツデータ {Dc} Kcの複製動作を説明するためのフローチャートである。

【0176】図17を参照して、携帯電話機100のユーザによって操作パネル1116から複製リクエストが入力されると(ステップS200)、コントローラ1120は、バスBS2を介して複製リクエストを受け、バスBS2およびメモリカードインタフェース1200を介して暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-infの出力要求をメモリカード110へ入力する(ステップS202)。

【0177】そうすると、メモリカード110においては、コントローラ1420は、端子1426、インタフェース1424、およびバスBS3を介して暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-infの出力要求を受理し(ステップS204)、バスBS3を介してメモリ1415から暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-infを読出し、その読出した暗号化コンテンツデータ {Dc} Kcおよび

付加情報Dc-infをバスBS3、インタフェース1424および端子1426を介して携帯電話機100へ出力する(ステップS206)。

【0178】携帯電話機100のコントローラ1120は、メモリカードインタフェース1200を介して暗号化コンテンツデータ {Dc} Kcおよび付加情報Dc-infを受理する(ステップS208)。そして、コントローラ1120は、メモリ1119から携帯電話機100のユーザの個人情報を読出し、暗号化コンテンツデータ {Dc} Kcに付加情報Dc-infおよび個人情報を付加して複製データを生成する(ステップS210)。具体的には、コントローラ1120は、暗号化コンテンツデータ {Dc} Kcを複製データ40の要素51に格納し、個人情報を要素53に格納し、付加情報Dc-infの内容をヘッダ50のコンテンツID501、コンテンツ名502、アーティスト名503、およびサイズ504に格納し、複製の日時をヘッダ50の日付505に格納して複製データを生成する。そして、コントローラ1120は、生成した複製データをバスBS2、送受信部1102、およびアンテナ1100を介して携帯電話機102へ送信する(ステップS212)。

【0179】携帯電話機102のコントローラ1120は、アンテナ1100、送受信部1102、およびバスBS2を介して複製データを受信し(ステップS214)、その受信した複製データを情報取得部1121に与える。情報取得部1121は、複製データから暗号化コンテンツデータ {Dc} Kc、付加情報Dc-inf、および個人情報を取得し(ステップS216)、暗号化コンテンツデータ {Dc} KcをバスBS2およびメモリカードインタフェース1200を介してメモリカード112へ入力する(ステップS218)。

【0180】メモリカード112においては、コントローラ1420は、端子1426、インタフェース1424およびバスBS3を介して暗号化コンテンツデータ {Dc} Kcを受理し、バスBS3を介してメモリ1415のデータ領域1415Cに暗号化コンテンツデータ {Dc} Kcを記録する(ステップS220)。

【0181】そして、携帯電話機100のコントローラ1120は、付加情報Dc-infおよび個人情報をメモリ1119に格納されたデータベース400に登録し(ステップS222)、携帯電話機100から携帯電話機102への暗号化コンテンツデータの複製動作が終了する(ステップS224)。

【0182】このように、暗号化コンテンツデータの複製においては、複製対象である暗号化コンテンツデータに複製元の個人情報を付加して複製先に送信し、複製元の個人情報が複製先において保持される。

【0183】なお、携帯電話機102のユーザは、携帯電話機100から受信した暗号化コンテンツデータ {D

c) Kcを復号および再生するためのライセンスを図7～図10に示すフローチャートに従って配信サーバ10から受信し、メモリカード112に格納する。これによって、携帯電話機100から複製された暗号化コンテンツデータ {Dc} Kcを復号および再生できる。

【0184】携帯電話機102のユーザは、携帯電話機100から複製された暗号化コンテンツデータを復号および再生する。そして、携帯電話機102のユーザは、その暗号化コンテンツデータが不用になったとき、メモリカード112から暗号化コンテンツデータを削除する。

【0185】しかし、携帯電話機102のユーザは、その削除した暗号化コンテンツデータが必要になるときがある。次に、携帯電話機102のユーザが、削除した暗号化コンテンツデータを携帯電話機100から再取得する動作について説明する。図18および図19は、携帯電話機102が携帯電話機100から暗号化コンテンツデータを再取得する動作を説明するための第1および第2のフローチャートである。

【0186】図18を参照して、携帯電話機102のユーザが操作パネル1116を介して複製元に関する情報の表示リクエストを入力すると（ステップS300）、携帯電話機102のコントローラ1120は、バスBS2を介して表示リクエストを受取り、 $n=1$ の設定を行なう（ステップS302）。そして、コントローラ1120は、メモリ1119に格納されたデータベース400の $n=1$ の欄に登録された複製元に関する情報を読み出し、その読み出した複製元に関する情報をバスBS2を介して表示パネル1118に与える。そして、表示パネル1118は、複製元に関する情報を画面60（図16参照）のフォーマットで表示する（ステップS304）。

【0187】携帯電話機102のユーザは、表示パネル1116に表示された複製元に関する情報を見て、複製を希望するとき再取得ボタン70を押し、複製を希望しないときキャンセルボタン71を押し。携帯電話機102のコントローラ1120は、再取得ボタン70が押された否かを判定し（ステップS306）、キャンセルボタン71が押されたときと判定したとき、 $n=n+1$ の設定を行ない（ステップS308）、ステップS304およびステップS306を繰返す。つまり、コントローラ1120は、 $n=2$ の欄に格納された複製元に関する情報をデータベース400から読み出して表示パネル1118に表示し、その表示した画面に基づいて暗号化コンテンツデータの再取得を行なうが否かの判定が行なわれる。

【0188】ステップS306において、コントローラ1120は、再取得ボタン70が押されたときと判定したとき、表示画面の電話番号に基づいて携帯電話機100へ電話を掛け、携帯電話機100と回線を接続する（ステップS310）。

【0189】そして、携帯電話機102のコントローラ

1120は、表示画面のコンテンツIDと、そのコンテンツIDによって特定される暗号化コンテンツデータ

{Dc} Kcの複製要求とをバスBS2、送受信部1102、およびアンテナ1100を介して携帯電話機100へ送信する（ステップS312）。

【0190】携帯電話機100においては、コントローラ1120は、アンテナ1100、送受信部1102、およびバスBS2を介してコンテンツIDと暗号化コンテンツデータの複製要求とを受信し（ステップS314）、受信したコンテンツIDによって特定される暗号化コンテンツデータの複製が可能か否かを判定する（ステップS316）。複製不可と判定されたとき、携帯電話機100のコントローラ1120は、複製不可のメッセージを送受信部1102およびアンテナ1100を介して携帯電話機102へ送信し、携帯電話機102は、複製不可のメッセージをアンテナ1100、送受信部1102、およびバスBS2を介して受信し、複製不可のメッセージを表示パネル1118に表示する（ステップS318）。そして、ステップS308へ移行し、ステップS304～S316が繰返される。

【0191】ステップS316において、携帯電話機100のコントローラ1120が複製可と判定したとき図19に示すステップS320へ移行する。図19を参照して、コントローラ1120は、コンテンツIDと、暗号化コンテンツデータの出力要求とをバスBS2およびメモリカードインタフェース1200を介してメモリカード110へ入力する（ステップS320）。

【0192】そうすると、メモリカード110においては、コントローラ1420は、端子1426、インタフェース1424、およびバスBS3を介してコンテンツIDと、そのコンテンツIDによって特定される暗号化コンテンツデータ {Dc} Kcの出力要求とを受理し（ステップS322）、バスBS3を介してメモリ1415からコンテンツIDによって特定される暗号化コンテンツデータ {Dc} Kcを読み出し、その読み出した暗号化コンテンツデータ {Dc} KcをバスBS3、インタフェース1424および端子1426を介して携帯電話機100へ出力する（ステップS324）。

【0193】携帯電話機100のコントローラ1120は、メモリカードインタフェース1200を介して暗号化コンテンツデータ {Dc} Kcを受理し、その受理した暗号化コンテンツデータ {Dc} KcをバスBS2、送受信部1102、およびアンテナ1100を介して携帯電話機102へ送信する（ステップS326）。

【0194】携帯電話機102のコントローラ1120は、アンテナ1100、送受信部1102およびバスBS2を介して暗号化コンテンツデータ {Dc} Kcを受信し、その受信した暗号化コンテンツデータ {Dc} KcをバスBS2およびメモリカードインタフェース1200を介してメモリカード112へ入力する（ステップ

S328)。

【0195】メモリカード112においては、コントローラ1420は、端子1426、インタフェース1424およびバスBS3を介して暗号化コンテンツデータ{Dc}Kcを受信し、バスBS3を介してメモリ1415のデータ領域1415Cに暗号化コンテンツデータ{Dc}Kcを記録する(ステップS330)。

【0196】その後、携帯電話機102のコントローラ1120は、暗号化コンテンツデータの複製が終了したか否かを判定し(ステップS332)、複製が終了していないとき図18に示すステップS304から図19に示すステップS332が繰返される。

【0197】ステップS332において、暗号化コンテンツデータの複製が終了したと判定されたとき、コントローラ1120は、その旨を表示パネル1118に表示し(ステップS334)、一連の動作が終了する(ステップS336)。

【0198】このように、携帯電話機102は、以前に複製した暗号化コンテンツデータの複製元の個人情報を保持することによって、暗号化コンテンツデータを携帯電話機100から容易に再取得することができる。

【0199】上記においては、暗号化コンテンツデータの複製に際して複製元である携帯電話機100が個人情報を複製対象である暗号化コンテンツデータに付加するとして説明したが(図17のステップS210参照)、本発明においては、複製元の個人情報は、複製先である携帯電話機102が作成してもよい。その場合、携帯電話機100から携帯電話機102への暗号化コンテンツデータの複製動作は、図20に示すフローチャートに従って行なわれる。図20に示すフローチャートは、図17に示すフローチャートのステップS210をステップS210aに代え、ステップS216をステップS216aに代え、その代えたステップS216aとステップS218との間にステップS217を挿入したものであり、その他は図17に示すフローチャートと同じである。

【0200】図20を参照して、上述したようにステップS200～S208が実行されると、携帯電話機100のコントローラ1120は、メモリカード110から受信した暗号化コンテンツデータ{Dc}Kcに付加情報Dc-infを付加して複製データを生成する(ステップS210a)。具体的には、コントローラ1120は、暗号化コンテンツデータ{Dc}Kcを複製データ40の要素51に格納し、付加情報Dc-infの内容をヘッダ50のコンテンツID501、コンテンツ名502、アーティスト名503、およびサイズ504に格納し、複製の日時をヘッダ50の日付505に格納する。

【0201】その後、上述したようにステップS212、S214が実行されると、携帯電話機102のコン

トローラ1120は、複製データを情報取得部1121に与え、情報取得部1121は、複製データから暗号化コンテンツデータ{Dc}Kcおよび付加情報Dc-infを取得する(ステップS216a)。そして、コントローラ1120は、複製元の電話番号(複製データの受信時に携帯電話機100から受信する)から携帯電話機100の個人情報を生成する(ステップS217)。その後、ステップS218～S224が上述したように実行され、暗号化コンテンツデータの複製動作が終了する。

【0202】このように、複製元が個人情報を暗号化コンテンツデータに付加しないとき、複製先が複製元の個人情報を作成して保持する。

【0203】図20に示すフローチャートに従って複製された暗号化コンテンツデータを複製元から再取得するとき、複製元に関する情報は、図16においてカード番号66およびE-mail67の部分が空白のまま表示される。これは、複製元である携帯電話機100から、携帯電話機100のユーザが所有するホームページのアドレスおよびカード番号が携帯電話機102へ送信されないからである。

【0204】暗号化コンテンツデータの複製および複製された暗号化コンテンツデータの再取得における複製先の携帯電話機102の機能ブロックを示すと図21に示すようになる。携帯電話機102は、コピー元情報取得部81と、コピー元情報管理部82と、コピー元情報表示部83と、コンテンツ再取得処理部84とを含む。

【0205】コピー元情報取得部81は、複製元である携帯電話機100から受信した複製データから暗号化コンテンツデータ{Dc}Kc、付加情報Dc-inf、および個人情報を取得し、その取得した付加情報Dc-infおよび個人情報をコピー元情報管理部に格納されたデータベース400に登録する。

【0206】コピー元情報管理部82は、図15に示すデータベース400を格納する。コピー元情報表示部83は、コピー元情報管理部82に格納されたデータベース400から複製元に関する情報を読み出し、その読み出した複製元に関する情報を表示する。コンテンツ再取得処理部84は、複製された暗号化コンテンツデータを複製元から再取得する処理を行なう。

【0207】したがって、図5に示す携帯電話機102の構成のうち、コントローラ1120および情報取得部1121は、コピー元情報取得部81を構成し、メモリ1119は、コピー元情報管理部82を構成し、表示パネル1118およびコントローラ1120はコピー元情報表示部83およびコンテンツ再取得処理部84を構成する。

【0208】上記においては、複製対象のコンテンツデータを公開鍵暗号方式によって配信サーバ10から携帯電話機100、102、104、106に配信された暗

号化コンテンツデータであるとして説明したが、本発明においては、複製対象のコンテンツデータは、インターネットを介して取得される暗号化されていないコンテンツデータであってもよい。すなわち、インターネットを介して携帯電話機へ配信されたコンテンツデータ、インターネットを介してパーソナルコンピュータへ配信されたコンテンツデータをケーブルを介して携帯電話機へ送信されたコンテンツデータ、およびパーソナルコンピュータがCDリッピングによって取得したコンテンツデータをケーブルを介して携帯電話機へ送信されたコンテンツデータ等が複製対象となる。つまり、コンテンツデータの取得経路は問わない。これらのコンテンツデータの複製および再取得の動作についても、図17～図20に示すフローチャートに従って行なわれる。

【0209】本発明の実施の形態によれば、コンテンツデータを複製するとき、複製先の携帯電話機は、複製元の個人情報を複製元の携帯電話機から受信して保持するので、その複製されたコンテンツデータを削除しても複製元の携帯電話機からその削除したコンテンツデータを容易に再取得できる。

【0210】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図5】 図1に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図6】 図1に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図7】 図1に示すデータ配信システムにおけるコンテンツデータの配信動作を説明するための第1のフローチャートである。

【図8】 図1に示すデータ配信システムにおけるコンテンツデータの配信動作を説明するための第2のフローチャートである。

【図9】 図1に示すデータ配信システムにおけるコンテンツデータの配信動作を説明するための第3のフローチャートである。

【図10】 図1に示すデータ配信システムにおけるコンテンツデータの配信動作を説明するための第4のフロ

ーチャートである。

【図11】 携帯電話機における再生動作を説明するための第1のフローチャートである。

【図12】 携帯電話機における再生動作を説明するための第2のフローチャートである。

【図13】 メモリカードにおける再生リストファイルの構成を示す図である。

【図14】 複製データのフォーマットである。

【図15】 複製元に関する情報を登録するデータベースを示す図である。

【図16】 コンテンツデータの再取得時に携帯電話機の表示パネルに表示される画面を示す図である。

【図17】 暗号化コンテンツデータの複製動作を説明するためのフローチャートである。

【図18】 複製された暗号化コンテンツデータを再取得する動作を説明するための第1のフローチャートである。

【図19】 複製された暗号化コンテンツデータを再取得する動作を説明するための第2のフローチャートである。

【図20】 暗号化コンテンツデータの複製動作を説明するための他のフローチャートである。

【図21】 コンテンツデータの複製動作および再取得動作を行なう携帯電話機の機能ブロックを示す図である。

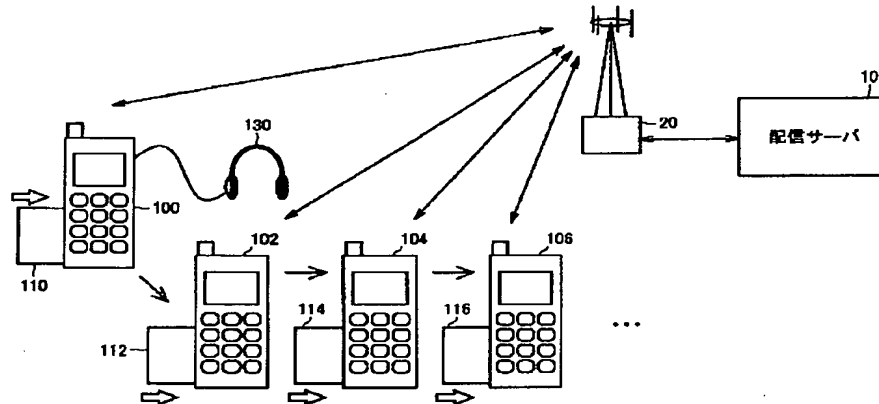
【符号の説明】

10 配信サーバ、20 配信キャリア、40 複製データ、50 ヘッダ、51～5n エレメント、60 画面、61 タイトル名、62, 501 コンテンツID、63, 503 アーティスト名、64, 504 サイズ、65 電話番号、66 カード番号、67 E-mail、68 コピー日時、69 その他、70 再取得ボタン、71 キャンセルボタン、81 コピー元情報取得部、82 コピー元情報管理部、83 コピー元情報表示部、84 コンテンツ再取得処理部、100, 102, 104, 106 携帯電話機、110, 112, 114, 116 メモリカード、130 ヘッドホン、160 再生リストファイル、350 通信装置、302 課金データベース、304 情報データベース、306 CRLデータベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312, 320, 1404, 1408, 1412, 1422, 1504, 1510, 1516 復号処理部、313 認証鍵保持部、315 配信制御部、316 セッションキー発生部、318, 326, 328, 1406, 1410, 1417, 1506 暗号処理部、400 データベース、502 コンテンツ名、505 日付、1120, 1420 コントローラ、1426, 1530 端子、1100 アンテナ、1102 送受信部、1104 マイク、1106 A

D変換器、1108 音声符号化部、1110 音声再生部、1112 DA変換器、1114 スピーカ、1116 操作パネル、1118 表示パネル、1119、1415 メモリ、1121 情報取得部、1200 メモリカードインタフェース、1400、1500 認証データ保持部、1402 Kmc保持部、1414 KPa保持部、1415A CRL領域、1415B ライセンス領域、1415C データ領域、141\*

\*6 KPmc保持部、1418 セッションキー発生部、1421 Km保持部、1424 インタフェース、1442、1446 切換スイッチ、1502 Kp1保持部、1518 音楽再生部、1519 DA変換器、1621~162n ライセンス管理ファイル、1611~161n コンテンツファイル、1550 コンテンツ再生デバイス。

【図1】



【図2】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例:音楽データ、朗読データ、教材データ、画像データ Kcにて番号可能な暗号化コンテンツデータ (DcKcとして配信され、メモリカードに保持される)
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
トランザクションID	ライセンス	ライセンス固有	配信を特定するための管理コード
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	トランザクションID+コンテンツIDの総称
ライセンス	ライセンス	ライセンス固有	Kc+ACm+ACp+ライセンスIDの総称
CRL	禁止クラスリスト	システム共通	使用禁止隠蔽データのリスト CRLの更新日(CRLdate)を含む

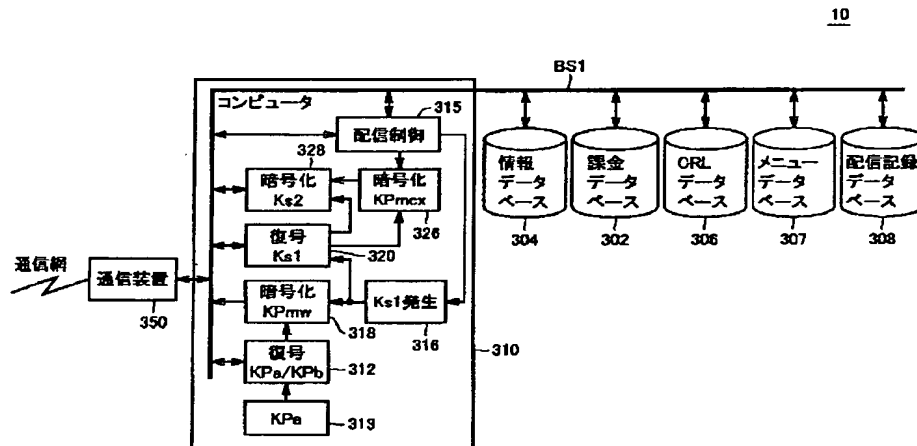
【図15】

コンテンツ番号	コンテンツ名	アーティスト名	サイズ	日付	電話番号	E-Mail	カード番号	その他
1								
2								
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
n								

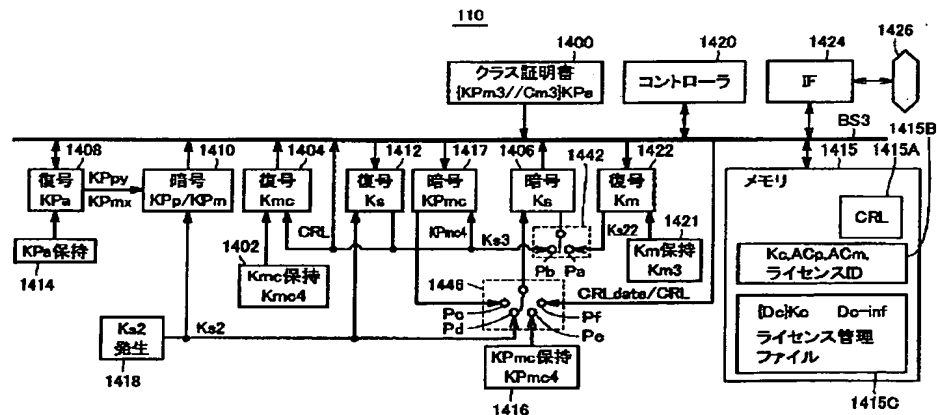
【図3】

	記号	種類	属性	特性
配信サーバ	KPa	公開鍵証明	システム共有	認証局にて認証データを復号する鍵
	Ka1	共通鍵	セッション固有	メモリカードへのライセンスの配信ごとに発生
メモリカード	KPa	公開鍵証明	システム共有	認証局にて認証データを復号する鍵 配信サーバのKPaと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ka2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受ごとに発生
	Cmw	証明書	クラス証明書	メモリカードのクラス証明書。認証機能を有する。 KPmw/CmwKPa又はKPmw/CmwKPaの形式で出荷時に記録。 *メモリカードのクラスwごとに異なる。
コンテンツ再生デバイス	KPpy	公開暗号鍵	クラス固有	証明書Cpyとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ka3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 KPpy/CpyKPaの形式で出荷時に記録。 *コンテンツ再生デバイスのクラスyごとに異なる。

【図4】

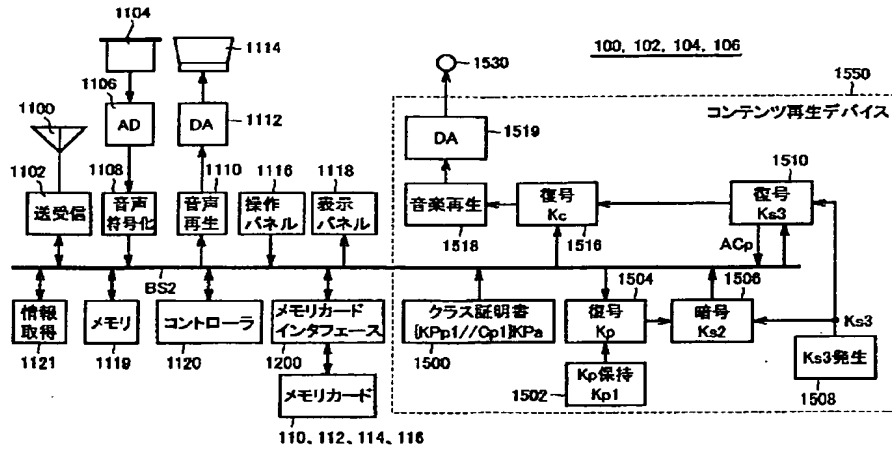


【図6】

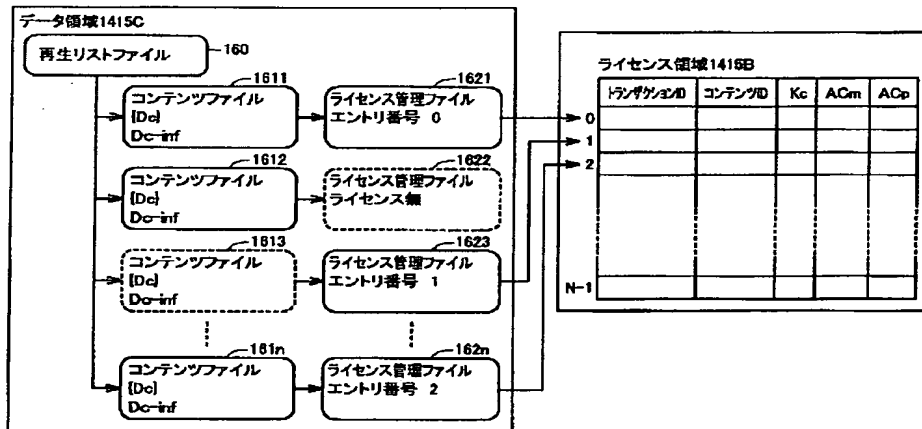




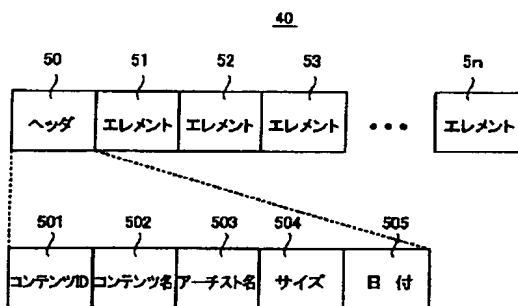
【図5】



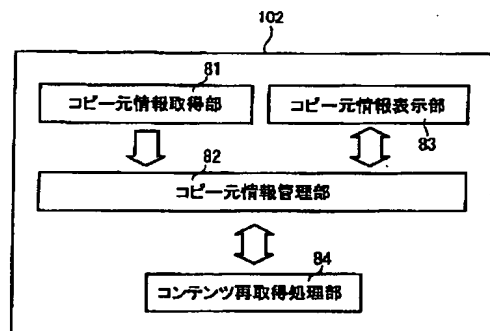
【図13】



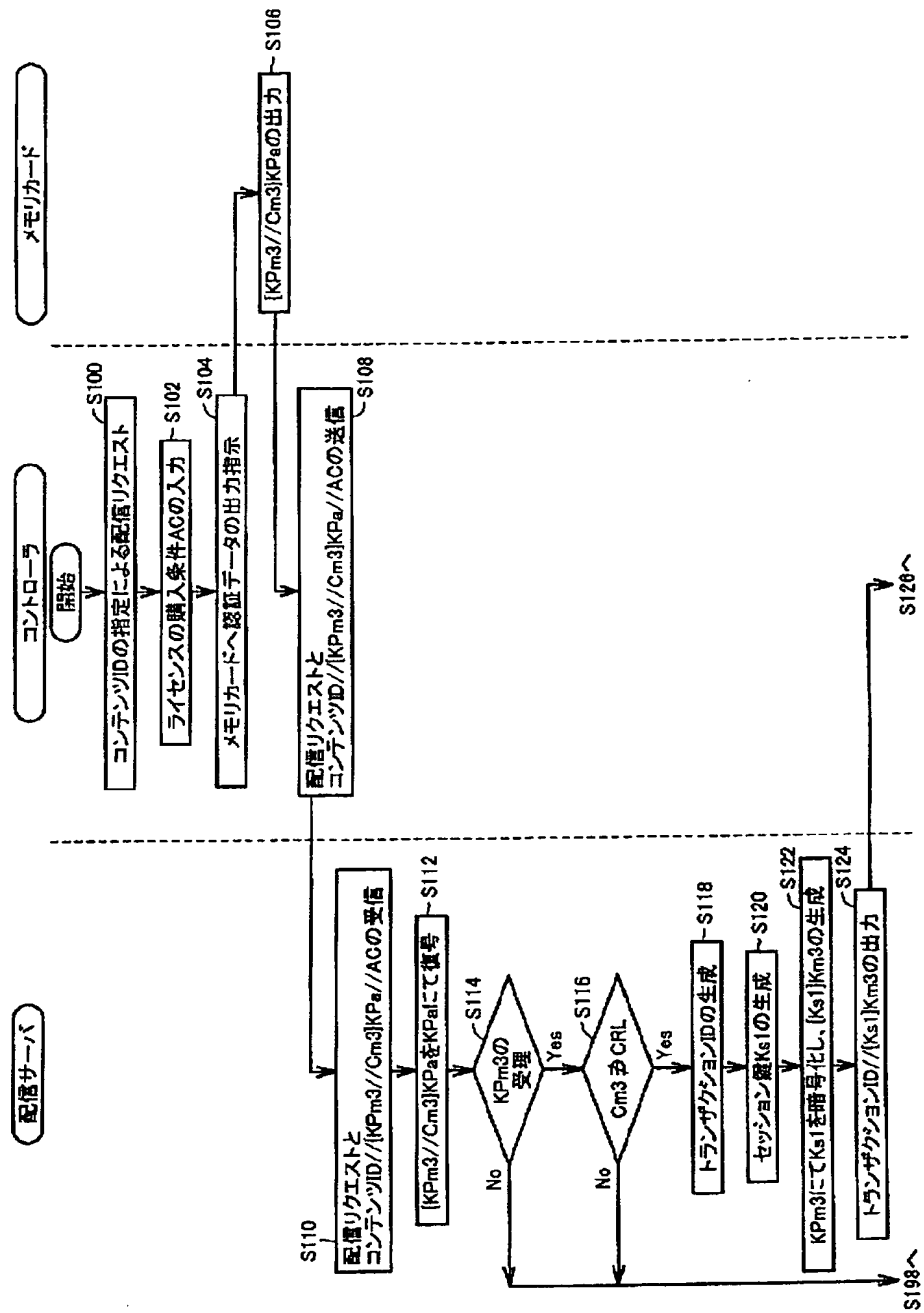
【図14】



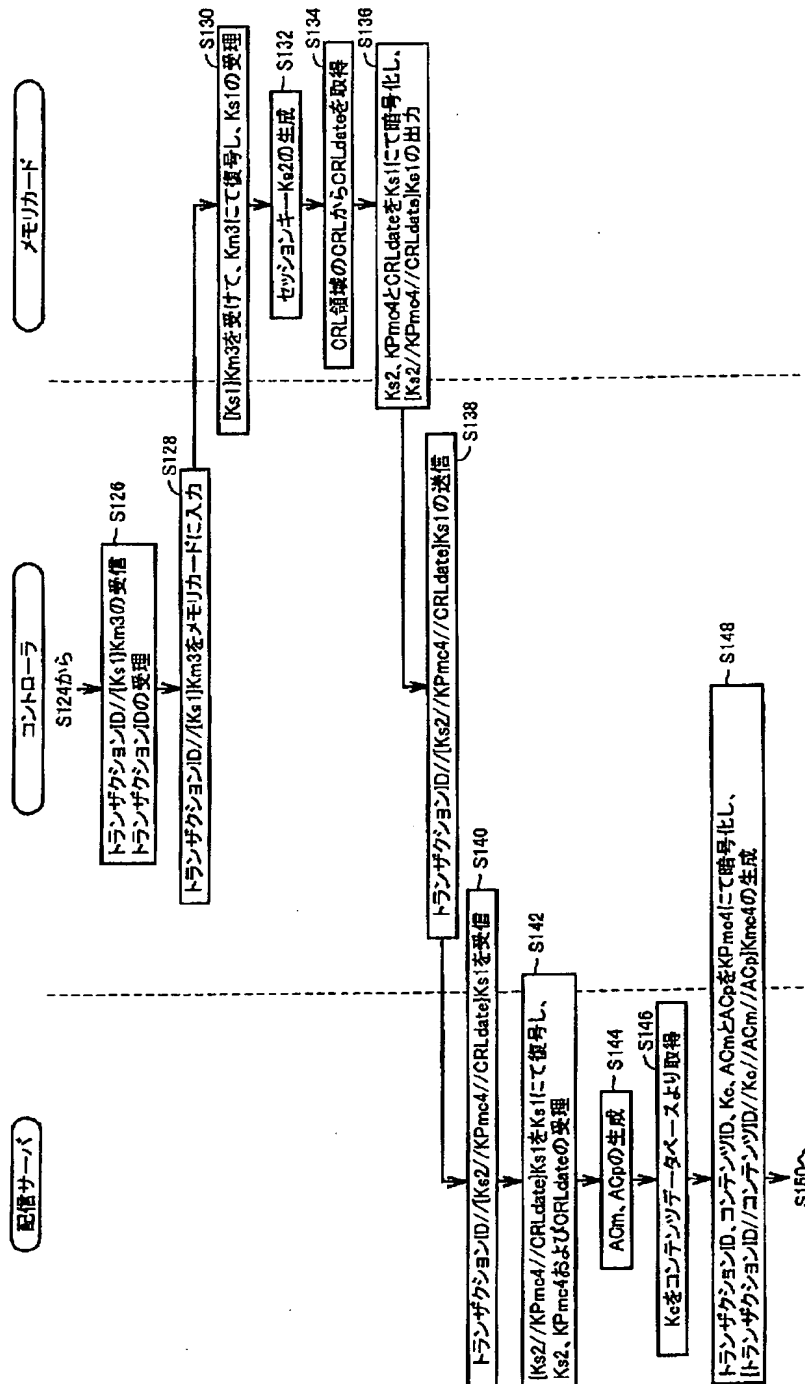
【図21】



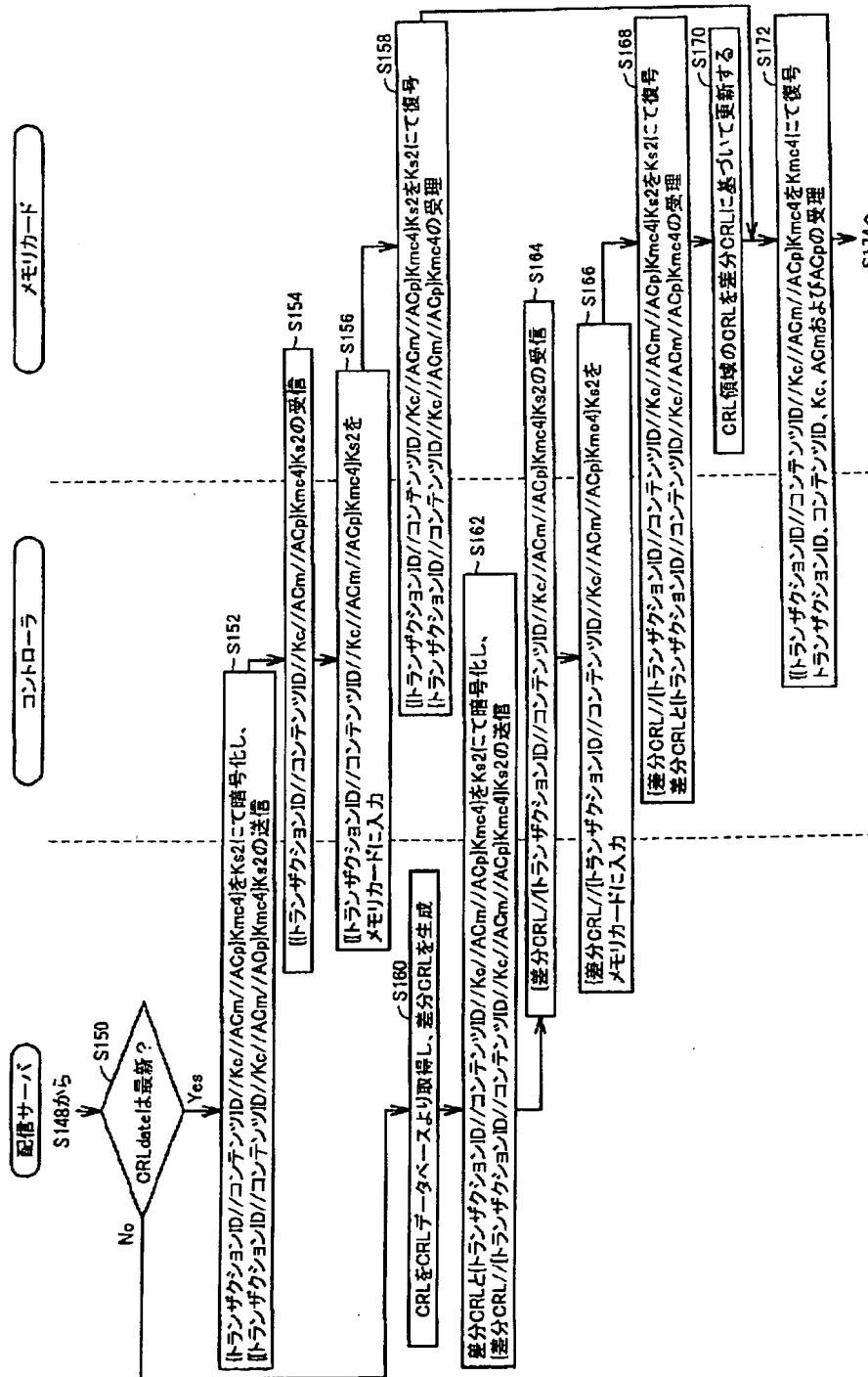
【図7】



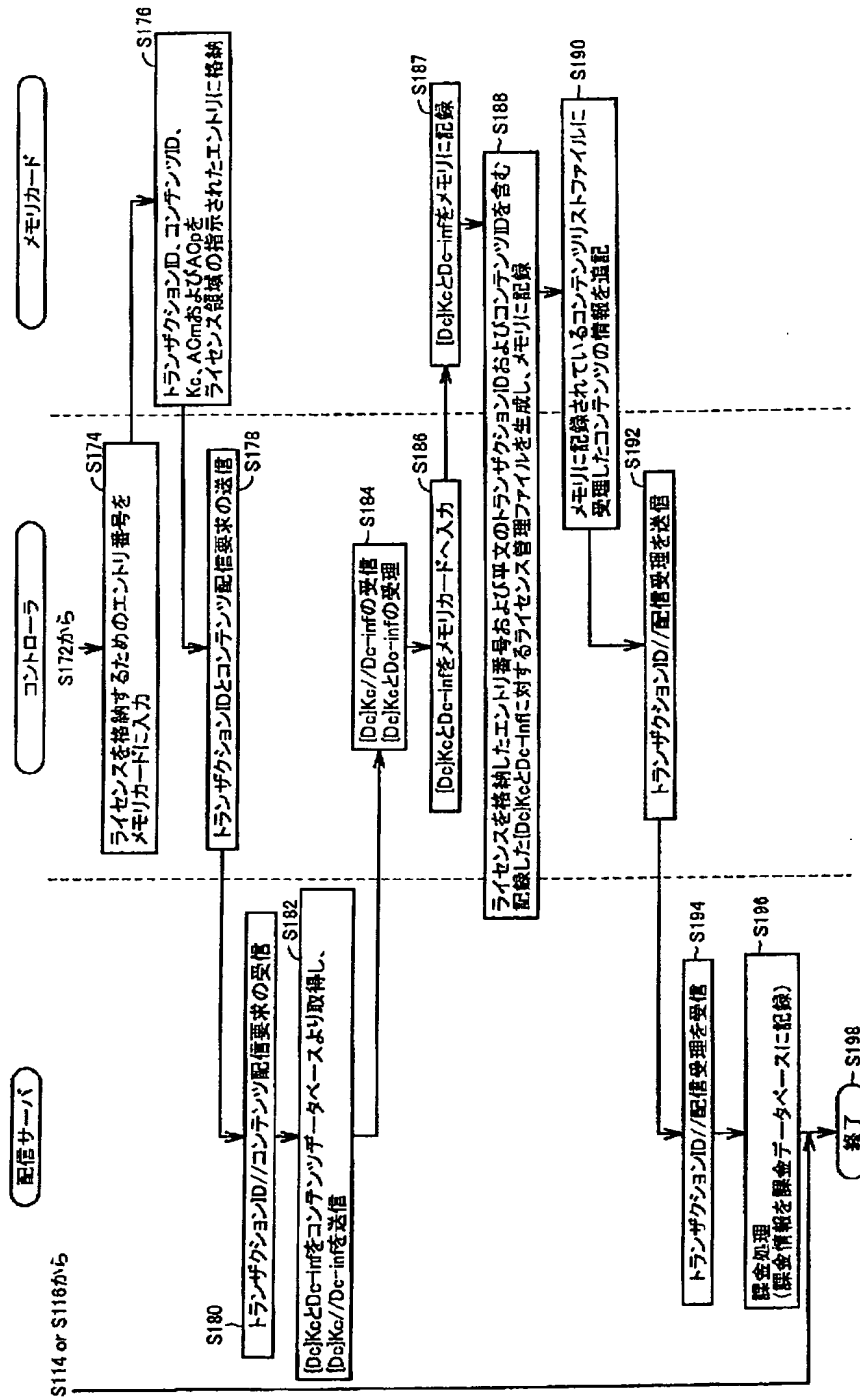
【図8】



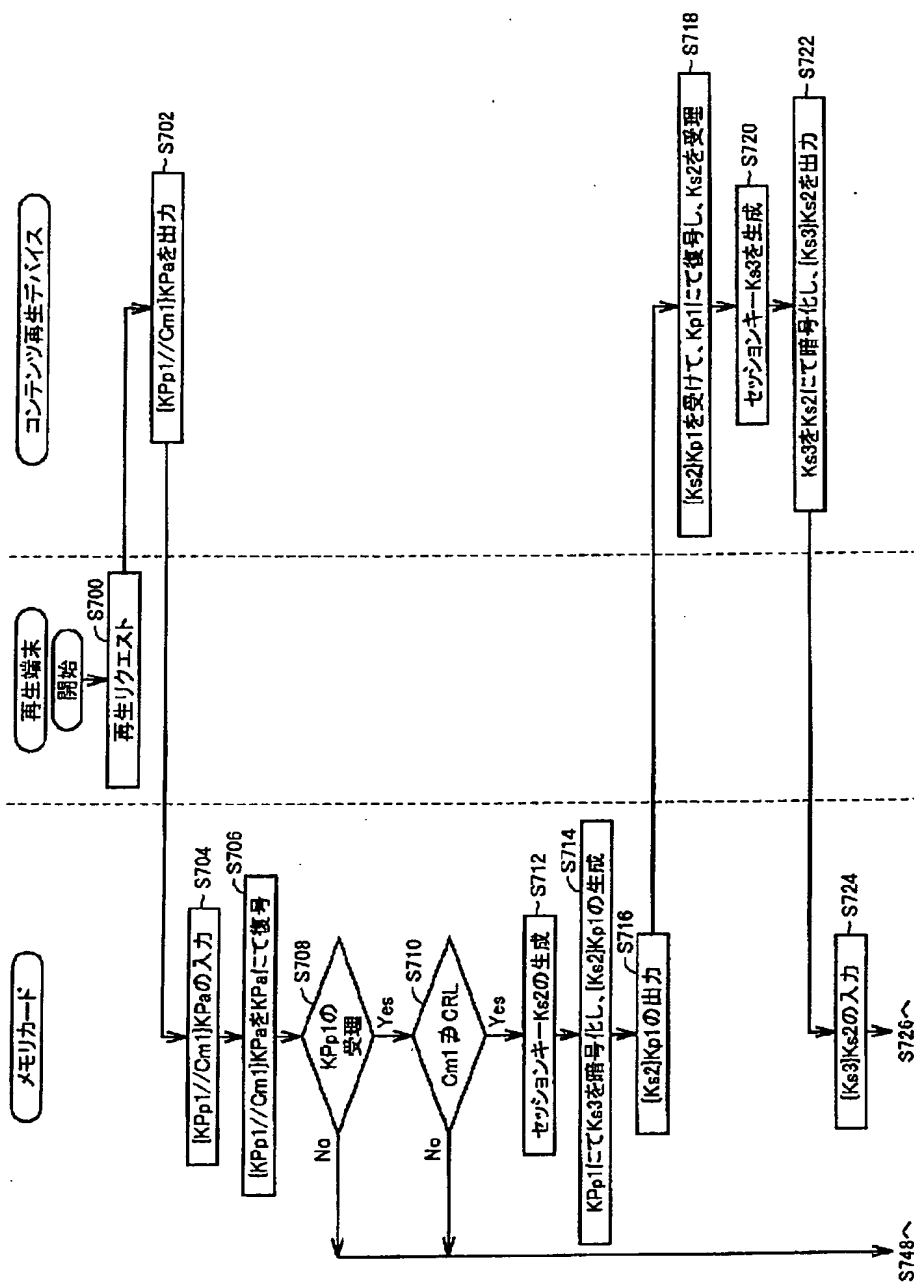
【図9】



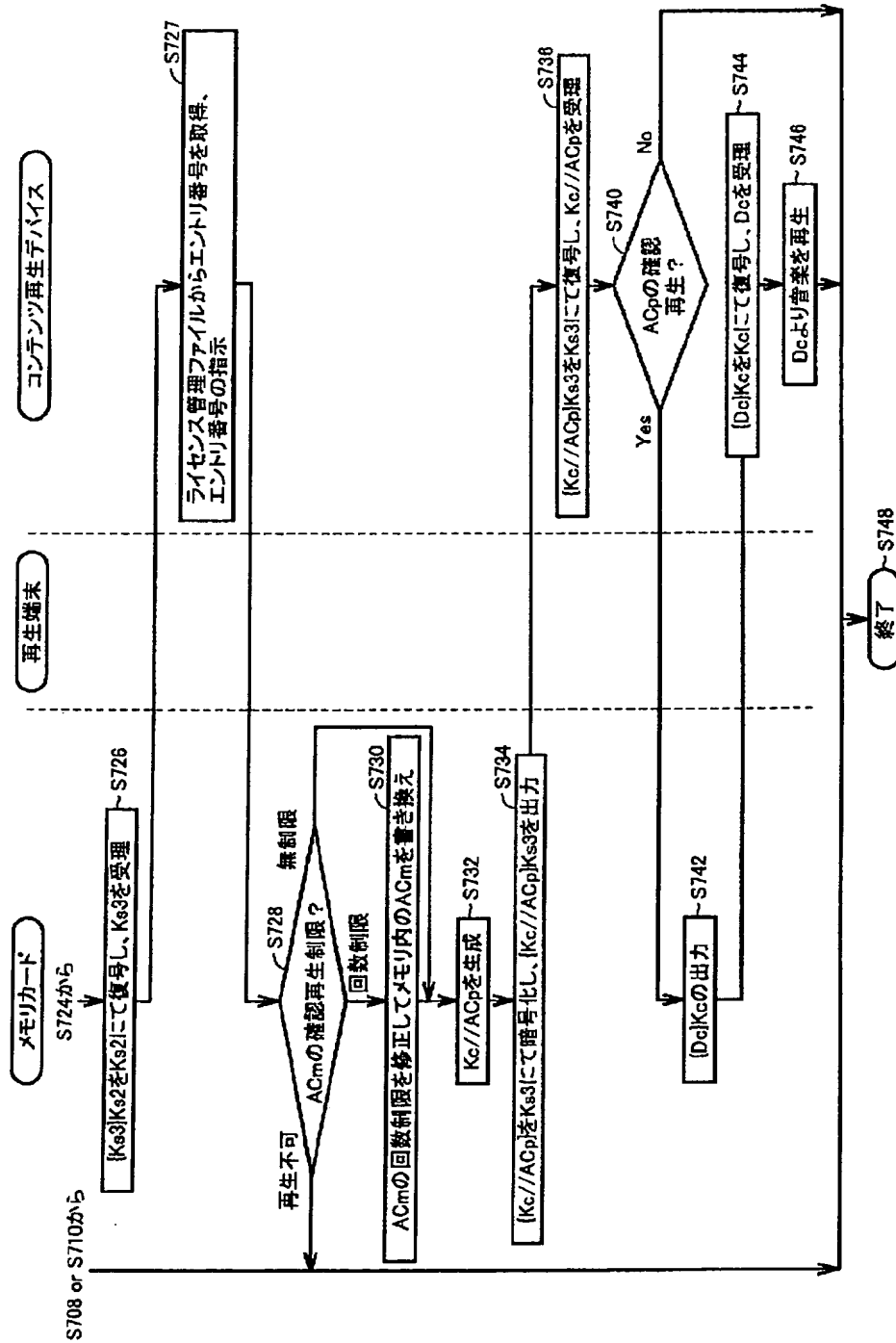
【図10】



【図11】



【図12】

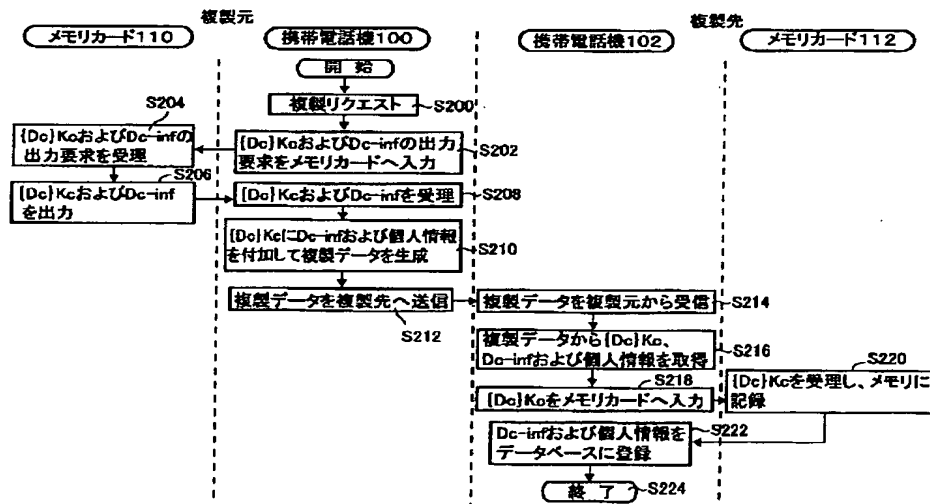


【図16】

60

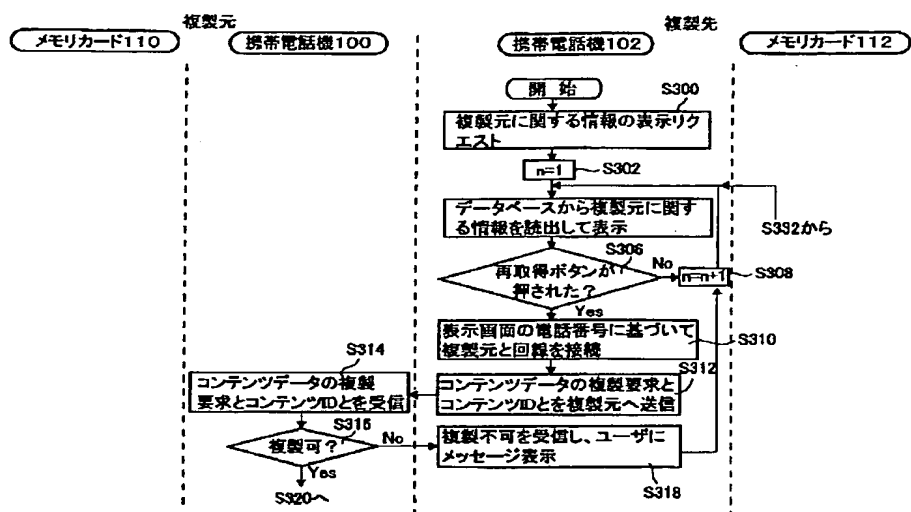
タイトル名: 61	アーティスト名: 63
コンテンツID: 62	サイズ: MB 64
電話番号: 65	カード番号: 66
E-mail: 67	
コピーした日時: 68	
その他: 69	再取得 70    キャンセル 71

【図17】

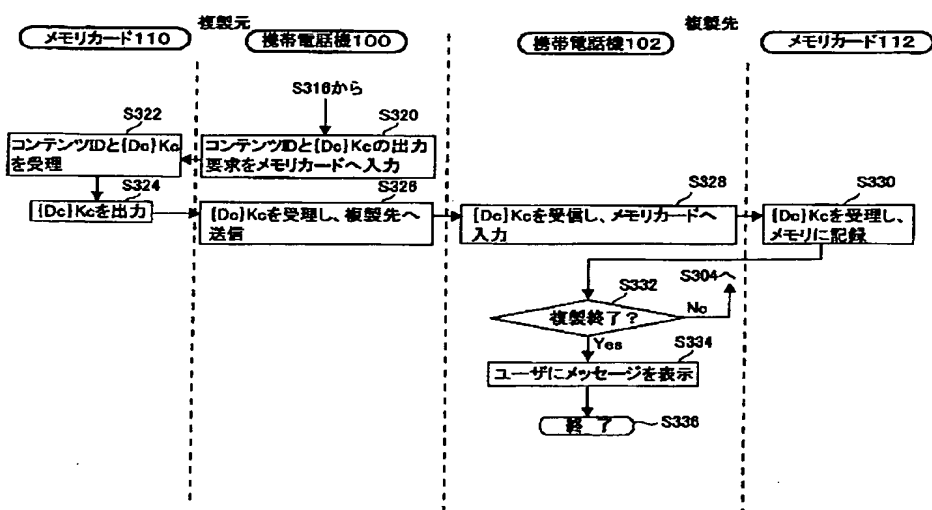




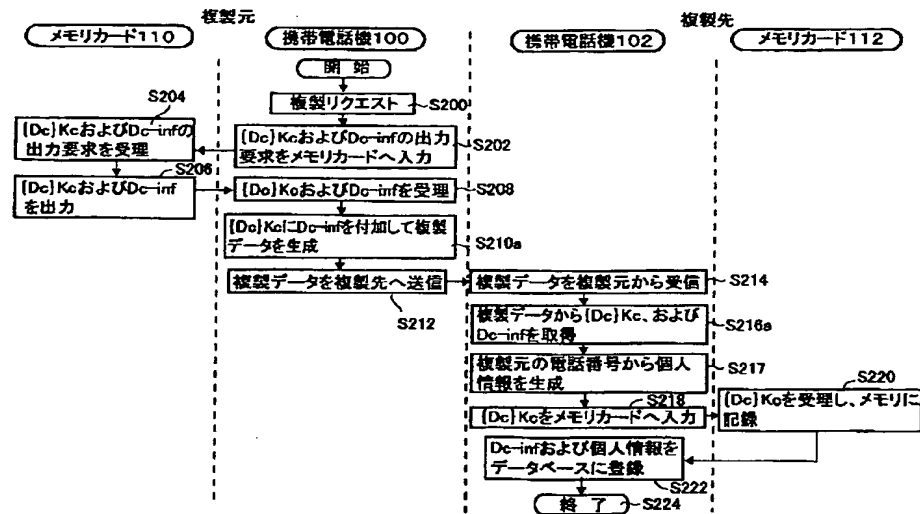
【图 18】



【图 19】



【図20】



フロントページの続き

(51)Int. Cl.<sup>7</sup>

G 1 0 K 15/02

H 0 4 L 9/08

識別記号

F I

G 1 0 K 15/02

H 0 4 L 9/00

テーマコード(参考)

6 0 1 B